Research Report of JFSA Multilateral Joint Research on the Chain of Trust of Decentralized Finance

June 2022
QUNIE Corporation

Background and purpose of this study

Decentralized financial systems based on blockchain technology enable Peer-to-Peer/Pool (P2P) financial transactions that reduce or eliminate the need for intermediaries and centralized processes. The financial services built primarily on public blockchains using smart contracts are called "DeFi (Decentralized Finance)". The crypto-asset market is currently growing rapidly, with TVL (Total Value Locked, the total value of crypto-assets deposited in a typical DeFi service) temporarily exceeding $100 billion[1] . On the other hand, DeFi is continuously experiencing fund theft due to smart contract vulnerabilities and theft of private keys, with the highest loss amount exceeding $600 million as of March 2022 (see 2-6-6), and the amount of damage when incidents occur is significant. Concerns have also been raised in terms of AML/CFT, user protection, and financial system stability.

Therefore, in this study, as part of the JFSA's "Multilateral Joint Research project", we conducted research on technical risks in the chain of trust (see 1-1-4) of decentralized financial systems, including DeFi. Although decentralized financial systems are considered to have decentralized and autonomous systems and governance as compared to existing financial systems, there are many DeFi that are considered to have multiple trust points (see 1-1-4). There are also some incidents in which the Weakest Link (see 1-1-5) among the components of DeFi was considered to be exploited. In addition, DeFi is now mainly operated by a Decentralized Autonomous Organization (DAO), but despite the name of DAO, there are some cases where it is believed that autonomous management is not being conducted but it is operated by a specific authority, and decision-making is conducted by a very small number of large governance token holders. Therefore, based on the assumption that the current major DeFi projects have certain trust points, we analyzed the case studies of representative DeFi projects; Uniswap (decentralized exchange: DEX), Maker (crypto-asset-backed stablecoin), and AAVE (lending), and their past incidents, and also interviewed the people involved in DeFi, in order to identify risks related to decentralized financial systems.

In general, entities trusted by users and other parties are subject to liability and may also be subject to regulation (e.g., banks). On the other hand, in DeFi, where parameter changes, smart contract upgrades, and decisions on use of funds are (to a certain extent) left to the community, decentralization of responsibility may make it difficult to identify regulatory targets, and a detailed trust point analysis for each project is considered necessary.[2] The DeFi is a decentralized financial system that is not only a financial institution, but also a community. In order for society as a whole to reap the fruits of innovation that a decentralized financial system can bring, it is important to identify and assess the risks of such a system and explore risk reduction measures with a view to the sound development of a decentralized financial system.

---

[1] DeFi pulse TVL(USD) 11/9/2021 9:00AM JST $110.26B https://www.defipulse.com/

[2] However, the transparency, autonomy, and tamper-resistance of blockchain may be utilized to reduce risk in a manner different from the traditional financial system, and traditional approaches to financial regulation may not necessarily be the optimal solution for decentralized finance as well. Based on objective analysis, this study focuses on providing a perspective from which regulators, developers, business stakeholders, and others can collaborate to solve the challenges of decentralized financial systems.

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

Background and purpose of this study 2
Acknowledgement 3
Disclaimer 3
Table of Contents 4
Glossary 6
Chapter 1. Getting the Big Picture on Chains of Trust for Decentralized Financial Systems 7
1-1 Main definitions for decentralized financial systems 7
1-1-1 Decentralized Financial System 7
1-1-2 DeFi (Decentralized Finance) 7
1-1-3 DAO (Decentralized Autonomous Organization) 7
1-1-4 Trust Point/ Chain of trust 8
1-1-5 Weakest Link 8
1-2 Key components of a decentralized financial system 8
1-3 Mapping of the main components that make up a decentralized financial system 13
1-3-1 Layering Concept 14
1-4 Analysis of technical characteristics of components per layer 16
1-4-1 Blockchain Infrastructure 16
1-4-2 Blockchain Infrastructure Extension Servise 19
1-4-3 Application Infrastructure and Applications 21
1-4-4 Aggregation 29
1-4-5 User and User Interface 29
1-5 Interoperability Analysis 30
Chapter 2. Analysis of Major DeFi Projects 31
2-1 Identification of DeFi projects to be studied 31
2-1-1 Selection of DeFi Projects to be Investigated (Decentralized Exchange) 31
2-1-2 Selection of DeFi Projects to be Investigated (Crypto-asset Stablecoin Issuance Platform) 33
2-1-3 Selection of DeFi projects for study (lending platform) 34
2-2 Analysis of the decentralized exchange Uniswap 35
2-2-1 Overall Project Overview 35
2-2-2 Main Technological Characteristics 39
2-2-3 Cooperation with Financial Institutions 44
2-2-4 Governance operations 45
2-2-5 Incident cases 49
2-2-6 Uniswap Main Trust Points 51
2-3 Stablecoin Maker (DAI) Analysis 53
2-3-1 Overall Project Overview 53
2-3-2 Main Technological Characteristics 57
2-3-3 Cooperation with financial institutions 68
2-3-4 Governance Operations 69
2-3-5 Incident Cases 74
2-3-6 Maker's main trust points 78
2-4 Lending Aave Analysis 79
2-4-1 Overall Project Overview 79
2-4-2 Main Technological Characteristics 83
2-4-3 Cooperation with financial institutions 90
2-4-4 Governance operations 91
2-4-5 Aave's main trust points 95
2-5 Results of Analysis of the Three Projects 97
2-5-1 Component Mapping of Major DeFi Projects 97
2-5-2 Comparison of Analysis Results for Surveyed Projects 99
2-6 Results of Major Incident Case Analysis of Other DeFi Projects 110
2-6-1 The DAO Attack 110

2-6-2 Flash Loan Attack #1 115
2-6-3 Flash Loan Attack #2 118
2-6-4 Money Laundering 120
2-6-5 Bitcoin Vulnerability (CVE-2018-17144) 123
2-6-6 Stealing of Funds Locked in a two-way Bridge in a Side Chain (Ronin Network) 125
2-6-7 Major Incident Cases after 2020 128
2-7 Analysis of Trust Point Weakest Link in Chains of trust 133
2-7-1 Analysis of Trust Points 133
2-7-2 Analysis of Weakest Link 135
Chapter 3. Identifying Risks in a Decentralized Financial System 139
3-1 Identifying Risk Factors in System Operation 139
3-2 Identifying Risk Factors in System Development 149
3-3 Identifying Risk Factors in Governance 154
3-4 Identifying Risk Factors in Engagement with Financial Markets 156
Chapter 4. Analysis of Risk Mitigation Measures in a Decentralized Financial System 159
4-1 Analysis of Risk Mitigation Measures in System Operation 159
4-2 Analysis of Risk Mitigation Measures in System Development 165
4-3 Analysis of Risk Mitigation Measures in Governance 169
4-4 Analysis of Risk Mitigation Measures in Engagement with financial markets 170
Conclusion 172

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 - A virtual machine that runs an Ethereum client (node)[3]
FATF	Financial Action Task Force
FISC	The Center for Financial Industry Information Systems
FSB	Financial Stability Board
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 - Customer verification program
TVL	Total Value Locked - Total value of crypto-assets deposited with DeFi

[3] Ethereum.org VIRTUAL MACHINE (EVM) https://ethereum.org/en/developers/docs/evm/

Chapter 1. Getting the Big Picture on Chains of Trust for Decentralized Financial Systems

This chapter shows the overall picture of chains of trust in the decentralized financial system (see 1-1-4) for the purpose of understanding how the decentralized financial system works. Specifically, we identify the major components that make up a decentralized financial system and organize them into a form that provides an entire perspective of the chains of trust by dividing the components into layers and mapping them as a whole.

This chapter is organized as follows: 1-1 defines key terms such as decentralized financial system, DeFi, DAO, and chains of trust; 1-2 describes the main components of them; 1-3 layers and maps the main components into layers to provide an overall picture of the chains of trust; and 1-4 describes the technical characteristics of the components by layer with specific examples. 1-5 describes the results of the interoperability analysis across the components between and within layers.

1-1 Main definitions for decentralized financial systems

1-1-1 Decentralized Financial System

The 2019 FSB report[4] 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.

1-1-2 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[5] . 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.

1-1-3 DAO (Decentralized Autonomous Organization)

There is no set definition of a decentralized autonomous organization (DAO) that operates a DeFi, but definitions have been attempted by Chohan[6] and Ethereum.org[7] in 2017, all of which focus on the organization's operations in a decentralized manner. In general, DAOs are considered to have the following characteristics compared to traditional corporations (e.g., joint stock companies).

<DAO features in major DeFi projects>

---

[4] Financial Stability Board: decentralised financial technologies: report on financial stability, regulatory and governance implications (2019). https://www.fsb.org/wpcontent/uploads/P060619.pdf

[5] Ryosuke Ushida and James Angel: Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs (2021). https://link.springer.com/chapter/10.1007/978-3-662-63958-0_2

[6] Definition of DAO by Chohan: Organization that is run through rules encoded as computer programs called “smart contracts”, WChohan, U.W.: The decentralized autonomous organization and governance issues. j. Cyber Policy 1-7 (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055

[7] Definition of DAO by Ethereum.org (a community run by the Ethereum Foundation): a member-owned community where centralized leadership is absent; a safe way to collaborate with strangers on the Internet; a safe place to entrust funds to a specific purpose https://ethereum.org/ja/dao/

- 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 one 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.

Based on the references and the MakerDAO case study, this report defines an organization as "a member-owned community where centralized leadership is absent and operations are conducted by rules encoded as computer programs (smart contracts)".

A well known example of a DAO in its early stage is "The DAO", an investment fund organization launched by the German company Slock.it in November 2015. "The DAO" was formed for profit and dissolved following a June 2016 fund leakage, but a DAO has since been introduced as a form of community management in numerous DeFi projects. In "The DAO," decision-making authority was concentrated in the hands of Slock.it, the operating company, and designated curators, but now, as in MakerDAO, there are moves to dissolve an operating company (such as Maker Foundation) and increase the degree of decentralization. However, there are many cases where an organization is called a DAO but is not actually operated autonomously.

1-1-4 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"[8].

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".

Also, the Single Point of Failure (SPoF) is used to describe the relationship between components, and is defined as "the part of a component of a system that, if it stops, will cause the entire system to stop"[9]. It often overlaps with the Trust Point.

1-1-5 Weakest Link

In this report, 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

A decentralized financial system consists of a variety of components, including not only the blockchain and smart contracts, but also the user interface, wallet, developer team, and infrastructure providers. This section provides an overview of each of the major components of a decentralized financial system, including their technical characteristics and their role in a decentralized financial system.

(1) Blockchain infrastructure

---

[8] Study Group on Digital and Decentralized Finance: Study Group on Digital and Decentralized Finance Interim Report https://www.fsa.go.jp/news/r3/singi/20211117/seiri.pdf

[9] What is JPNIC SPOF https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1667.html

The following blockchains are used as the basis for structuring DeFi.

a. Main chain (e.g. Ethereum)

It is the base blockchain for running the DeFi protocol and is the parent chain for sidechains and Layer 2 scaling solutions. The main chain generally has the following characteristics (described primarily with Ethereum in mind)

- Flexible smart contract functionality for deploying DeFi protocols.
- The client (node) shares blocks and other data via a peer-to-peer (P2P) network between nodes. Clients (nodes) are equipped with virtual machines (EVM) to execute smart contracts
- There are two types of accounts held in the blockchain.
  - Externally Owned Accounts (EOAs) are 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).
  - The contract account is the deployed smart contract account, and smart contracts are executed in response to the receipt of messages from EOAs or other contract accounts.
- The clients (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) necessary to execute smart contracts.
- A large number of DeFi are running on the main chain, and the increase in the number of users has caused problems such as the transaction execution fee (gas price) to skyrocket and transaction congestion, which makes code execution (incorporation into the block, which is a prerequisite for code execution) time consuming.
- Recently, emerging chains such as Avalanche and Solana have appeared on the market, and their market share has been changing to some extent.
- There is also a hierarchical chain[10] that scales up the main chain and is considered to have interoperability and scalability.

b. Side chain[11] (e.g. Polygon)

It is 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, and generally has the following characteristics

- While main chain's consensus algorithms (e.g. Ethereum currently uses PoW: Proof of Work) are often energy intensive and limited in processing speed, sidechains can reduce power 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.
- It is connected to the main chain by a two-way bridge[12] . When funds are exchanged between the main and side chains, funds are locked in the two-way bridge to prevent double spending.
- Some sidechains are based on the same virtual machine as the main chain (e.g., EVM), in which case the same programming language and libraries function in the sidechain as in the main chain (Ethereum).
- There are generally two types of accounts held in the sidechain: externally owned accounts and contract accounts, as in the main chain.

[10] Tiered Chain: A blockchain with a unique network structure that includes a main chain and individual subchains connected to it, such as Polkadot. The subchain executes smart contracts, while the main chain relays messages.

[11] Ethereum.org SIDECHAINS https://ethereum.org/en/developers/docs/scaling/sidechains/

[12] Ability to exchange tokens between main and sidechains Ethereum.org Blockchain bridges https://ethereum.org/en/bridges/

(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.

*Rollup[13] : 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.

a. Optimistic Rollup[14]

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. It also inherits Ethereum's security. When a write is made to the Ethereum main chain, the validity of the written data is not verified. Instead, Fraud-Proof allows a challenge to be filed if the verifier detects an unauthorized state transition during the challenge period (basically 7 days).

b. zk-Rollup (Zero Knowledge Rollup)[15]

zk-Rollup combines hundreds of transactions into one off-chain transaction and generates a cryptographic proof of validity of the transaction data. Because only the validity proofs of validity are sent to the Ethereum main chain, rather than all transaction data, the data contained is said to be smaller, making block verification faster and cheaper.

Since zk-Rollup verifies the validity of data at the time of writing to the main chain, there is no fraud verification delay in transferring funds from Layer 2 to Layer 1, as in Optimistic Rollup.

(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.

(4) Smart Contracts[16]

Smart contracts are generally rules (contracts) that are written as programs and automatically executed and processed on the blockchain (distributed ledger). On Ethereum and similar "blockchain infrastructure" they mean code (functionality) and data (state) that resides at a specific address on the blockchain.

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.

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.

In addition, 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).

---

[13] LAYER 2 ROLLUPS https://ethereum.org/ja/developers/docs/scaling/layer-2-rollups/

[14] Ethereum.org OPTIMISTIC ROLLUPS https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/

[15] Ethereum.org ZERO-KNOWLEDGE ROLLUPS https://ethereum.org/en/developers/docs/scaling/zk-rollups

[16] Ethereum.org INTRODUCTION TO SMART CONTRACTS https://ethereum.org/ja/developers/docs/smart-contracts/

In this report, the smart contracts that enable DeFi functions and services are referred to as "DeFi protocols". Strictly speaking, the DeFi protocol consists of a smart contract that runs on the blockchain and the DeFi protocol interface that allows users to operate the smart contract from the outside. The DeFi protocol interface refers to the DeFi protocol operation screen and information displayed in a web browser.

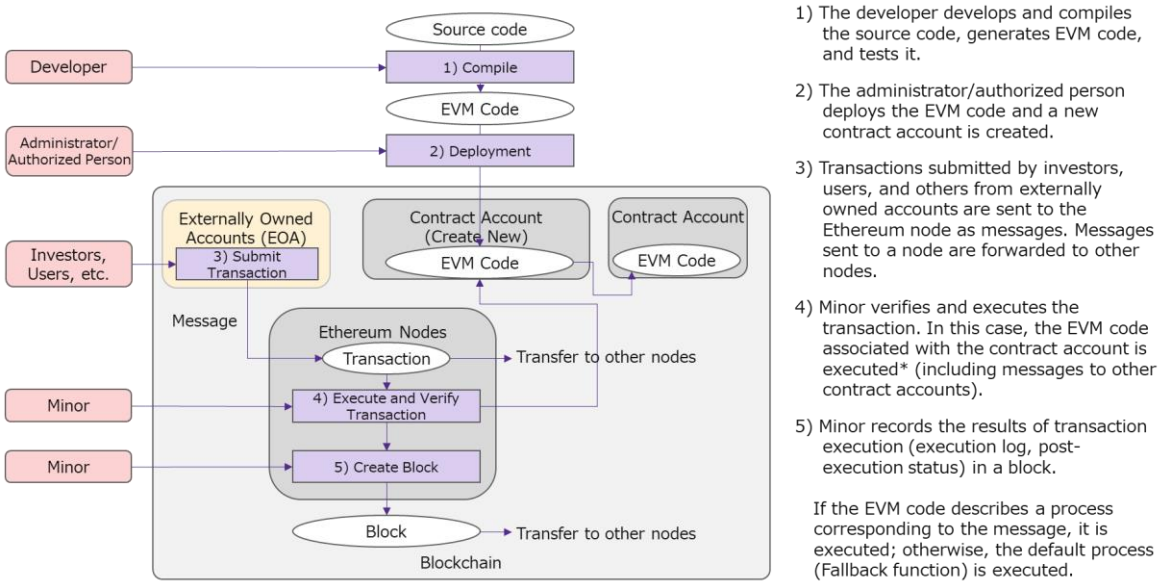


Figure 1-2 Flow of smart contract execution (in Ethereum)

(5) Wallet

The 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.

<About the private key>

In ISO/IEC20008-1[17] , the key used for signing and verification with public key cryptography is called the signing key (private key) and the key used for verification is called the verification key (public key). In this report, they are referred to as private key and public key, respectively.[18] IPA explains thet in public key cryptography, two keys (private key and public key) are used in pairs. In digital signatures, a message is encrypted using a private key, which is then verified using the public key of the pair to ensure the integrity of the message and the authentication of the signer (see 1-2(6)).

a. Cold wallet

Cold wallets manage users' private keys in a completely isolated state from the Internet using paper wallets or dedicated hardware wallets. Therefore, cold wallets are generally less convenient than hot wallets, but they are considered more resistant to attacks via the network, and are used for storing high-value crypto-assets at crypto-asset exchanges, etc.

b. Hot Wallet[19]

[17] ISO/IEC 20008-1:2013(en) Information technology - Security techniques - Anonymous digital signatures Part 1: General https://www.iso.org/obp/ui#iso:std:iso-iec:20008:-1:ed-1:v1:en

[18] 2.2 Public Key Cryptography 2.1 Overview https://www.ipa.go.jp/security/pki/022.html

[19] FSA Summary of FATF Report to G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins (Provisional Translation) (7/2020) https://www.fsa.go.jp/inter/etc/20200701.pdf

Hot wallets are classified into the following two categories based on the location of the user's private keys.

- Unhosted wallet
  Unhosted wallets are generally defined as wallets where the private key is managed directly by the user who is the holder of the wallet, and the user can directly perform crypto-asset transfer transactions, etc. Unhosted wallets use Ethereum libraries such as web3.js to connect directly to the Ethereum blockchain.
- Hosted wallet
  In hosted wallets, users entrust the management of their private keys to a wallet administrator (host/custodian) such as a cryptocurrency exchange, and users cannot directly execute crypto-asset transfer transactions.

(6) User Interface

The IPA defines a user interface as "a point where a user, a device, and system interact when the user uses the device system"[20] . In DeFi, it refers to the user authentication[21] 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 providers

Infrastructure providers are 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.

Development tool features include developing/debugging smart contracts, compiling source code, testing on local nodes, and deploying to the blockchain for developement. Some development tools utilize the capabilities of infrastructure providers, such as Infura.

(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[22]

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), and so on.

---

[20] IPA Quality at the Point of Use" in a Connected World https://www.ipa.go.jp/files/000057850.pdf

[21] User authentication is a system for identifying users to a system or application. This system can be used to control access to specific information and protect information. The most common method is to use "multi-factor authentication," in which a user is authenticated by a combination of several of the following factors

- Only known to the user (password)
- Items owned by the user (keys, cards, smart phones, phones, etc.)
- Representation of user characteristics (biometrics such as fingerprints)

[22] Ethereum.org SPIN UP YOUR OWN ETHEREUM NODE https://ethereum.org/ja/developers/docs/nodes-and-clients/run-a-node/

(11) Oracle[23]

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. There are cases where multiple external feeds are set up by self to obtain external market prices (Maker), and cases where external decentralized oracle services such as Chainlink are used (Aave).

(12) Governance token/ Governance vote

Although there is no strict definition of a governance token, it generally refers to a token that is granted the right to vote on community decisions, such as modifying the functionality of the DeFi protocol, changing parameters such as additions and interest rates, and using community funds, by the governance token holders. A mechanism whereby holders vote according to rules determined by the amount held and implement what is passed is often referred to as "governance voting".

(13) KYC certified 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) Aggregators[24]

It refers to 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.

DeFi aggregators find optimal token exchange rates and yields from decentralized exchanges, lending protocols, liquidity pools, etc. and offer them on their platforms.

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

The overall mapping was based on the key components outlined in 1-2 and the dependencies in DeFi's chain of trust

In this report, the analysis is conducted with Ethereum in mind as the blockchain infrastructure, and the relationship with other main and side chains is specified in each case. In addition, although the mapping is divided into layers to clarify the dependencies of the chain of trust, it should be noted that the trust and security relationships of the components may in fact span the entire layer, and the division into layers does not mean that the target is limited to a specific layer.

[23] Ethereum.org ORACLES https://ethereum.org/ja/developers/docs/oracles/

[24] DeFi Aggregator https://coinmarketcap.com/alexandria/glossary/defi-aggregator

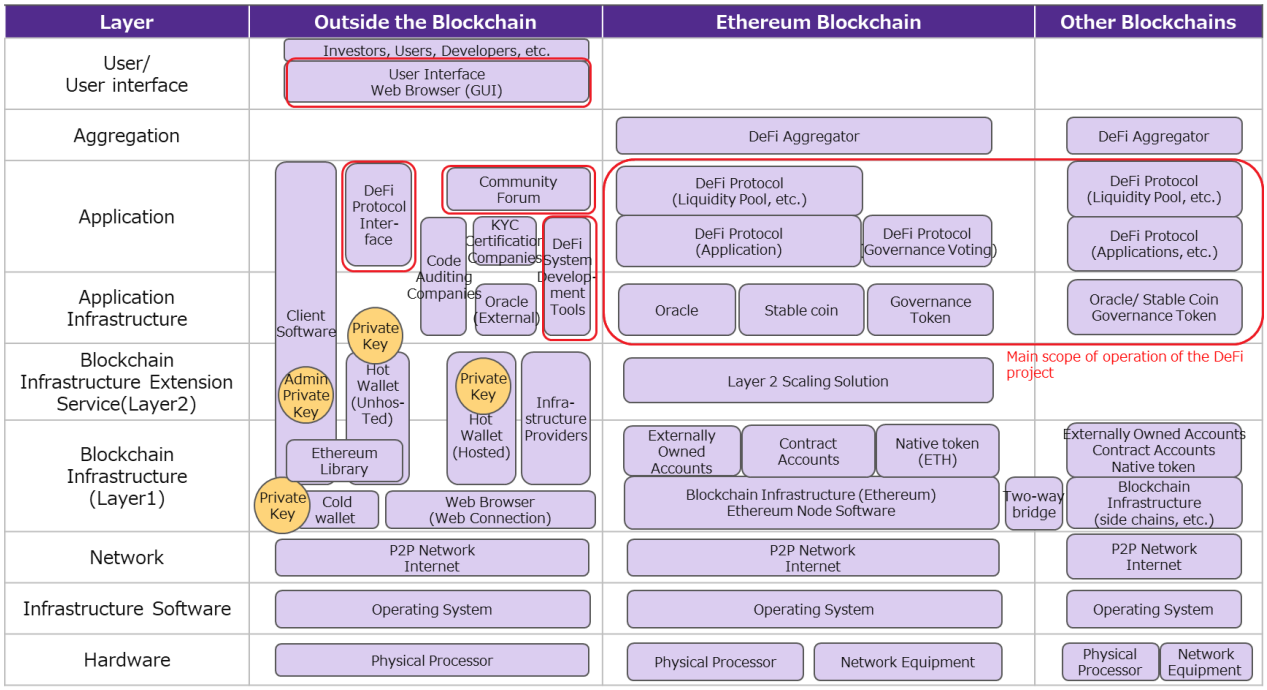


Figure 1-3 Mapping of the main components of a decentralized financial system

1-3-1 Layering Concept

For the purpose of placing the dependencies between components up and down between layers, the following concept is used to classify the layers in which the major components are placed.

(1) Hardware/ Infrastructure software layer

Place hardware and operating system, Internet, and P2P Network for the blockchain.

(2) Blockchain infrastructure (Layer 1) layer

The main chain (Ethereum), which is the blockchain infrastructure, as well as side chains and hierarchical chains are placed. Externally owned accounts, contract accounts, and native tokens are also placed in this layer as they are part of the blockchain functionality.

Sidechains are placed in parallel with the Ethereum blockchain as they connect with the main Ethereum chain via a two-way bridge and operate independently of Ethereum.

Outside of the blockchain are infrastructure providers that work with the blockchain infrastructure, cold and hot wallets that work with externally owned and contracted accounts, and client software.

(3) Blockchain Infrastructure Extension Service (Layer 2) Layer

Layer 2 scaling solutions that run dependent on the blockchain infrastructure is placed in this layer.

In addition, since infrastructure providers, unhosted wallets, wallet administrators, and client software are related to both layers 1 and 2, they are placed across both layers.

(4) Application Infrastructure Layer

Oracles, stabled coins, and governance tokens that are normally required for application layers such as the DeFi protocol (smart contracts) are placed.

Outside of the blockchain, an external oracle that works with the Oracle, DeFi system development tools to develop the application infrastructure, etc. are placed.

(5) Application layer

The application layer contains the DeFi protocol (smart contract) applications (various DeFi functions and services, etc.).

Outside of the blockchain, the DeFi protocol interface, that work with the DeFi protocol, community forums, client software, DeFi system development tools, etc. are placed.

(6) Aggregation layer

The aggregation layer includes a DeFi aggregator that aggregates multiple DeFi projects. (Components outside the blockchain of the DeFi Aggregator are omitted as the mapping shows the dependencies of the DeFi projects.)

(7) User/User Interface Layer

User interface between the user and other components is placed in this layer.

1-4 Analysis of technical characteristics of components per layer

1-4-1 Blockchain Infrastructure

An overview and key technical characteristics are described for the following blockchain infrastructures.

(1) Overview and technical characteristics of the blockchain infrastructure

Table 1-4-1 Technical characteristics of the blockchain infrastructure

Blockchain (Native Token)	**Ethereum (ETH)**	**Polygon (MATIC)**	**Avalanche (AVAX)**	**BNB Smart Chain (BNB)**	**Polkadot (DOT)**
Classification.	main chain	side-chain	main chain	main chain	main chain (hierarchical chain)
Summary	- Numerous DeFi and smart contracts are being built. - Migration to Eth 2.0 is underway in stages to resolve scalability and other issues.	- Sidechain of Ethereum, compatible with EVM[25] - High processing speed and low remittance fees due to scaling technology	- Low remittance fees with scaling technology - Compatible with Ethereum and EVM	- Low remittance fees with scaling technology - Compatible with Ethereum and EVM - Consensus algorithm with fixed 21 validators for high speed processing	- Aim to build a highly interoperable infrastructure by connecting the main chain (relay chain) and the para-chains (individual blockchains that scale up).
Service Launch	2015	2017	2020	2019	2017
Founder	Vitalik Buterin	Jaynti Kanani (CEO) Sandep Nailwal, Anurag Arjun	Emin Sirer (Professor at Cornwell)	Changpeng Zhao (CEO of Binance Exchange)	Dr. Gavin Wood (Co-founder of Ethereum)
Development team, etc.	Ethereum Foundation	Polygon Technology	Ava Labs	Binance Holdings Ltd.	Web3 Foundation

[25] In this table, "compatible" means that Ethereum smart contracts will run on other blockchains.

Consensus algorithm	GHOST[26] (Proof of Work) Eth2.0: Proof of Stake in transition	Proof of Stake	Proof of Stake	Proof of Staked Authority (PoSA)[27]	Nominated Proof of Stake (NPoS)
Smart Contract Development Language[28]	Solidity, Vyper	Solidity, Vyper	Solidity, Vyper	Solidity, Vyper	Solidity, Vyper
Throughput	15TPS	65,000TPS	400-1,500TPS	10,000TPS	1,000TPS
Execution model (machine)	Account-Based[29] (EVM)	Account-Based (EVM)	UTXO-Based[30] (AVM+EVM+more)	Account-Based (EVM)	Account-Based
Avarage block generation time[31]	14sec.	2sec[32]	2sec	5sec.	6sec.
Major Token Standards	ERC-20, ERC-721, ERC-1155	ERC-20, ERC-721, ERC-1155	ERC-20, ERC-721, ERC-1155	BEP-20, BEP-721, BEP-1155	-
Major Stablecoins	USDT, USDC, DAI, TerraUSD	USDT, USDC, DAI, TerraUSD	USDT, DAI, TUSD, TerraUSD	DAI, BUSD, TerraUSD	USDT, USDC, sUSD, TerraUSD
Major DeFi Services	Uniswap, Maker, Aave	Uniswap, Maker, Aave	Maker, Aave, Pangolin	Maker, Aave, Pancake Swap	Reef, Curve
Major NFT Services	Flow, Enjin, Mana, Opensea	Polygonpunks, Opensea	NFTrade, Kalao	Juggerworld, Treasureland	Bondly, Xen
Major Wallet	Metamask, Trust wallet	Metamask, Coinbase Wallet	Avalanche wallet, Metamask	Metamask, Trust Wallet	Polka Wallet, Trust Wallet

[26] GHOST (Greedy Heaviest Observed Subtree): A mechanism that makes the chain with the most accumulated calculations the correct chain.

[27] PoSA:PoS (Proof of Stake) combined with PoA (Proof of Authority) Binance Smart Chain What is Binance Smart Chain? https://docs.binance.org/faq/bsc/bsc.html

[28] https://chainstack.com/protocols/ethereum/

[29] Account-Based: A method of managing and recording account balances as data, just like a bankbook.

[30] UTXO-Based (Unspent Transaction output): Method to calculate and obtain the address balance based on transaction data only

[31] Solana comparison to other chains https://www.reddit.com/r/solana/comments/qpt2bb/solana_comparison_to_other_chains/

[32] Polygon PoS Chain Average Block Time Chart https://polygonscan.com/chart/blocktime

[Column: Ethereum 2.0 Sharding[33]]

Sharding is a multi-phase upgrade to improve Ethereum's scalability and capacity. This upgrade is expected to be released in 2023. Features of sharding as follows.

- Sharding is the process of horizontally partitioning a database to distribute the load, reducing network congestion and increasing transactions per second by creating new chains called "shards.
- The shard chain distributes the network load across 64 new chains and low hardware requirements, making it easier for nodes to run.
- In a shard chain, the validator only needs to run or maintain shards, which are small pieces of data, and does not need to validate the entire network. This speeds up processing and reduces hardware requirements.
- Sharding is said to eventually allow people to run Ethereum on their personal PCs and smartphones without having to rely on intermediary services. It is expected that more people will be able to participate as clients and execute transactions on sharded Ethereum.

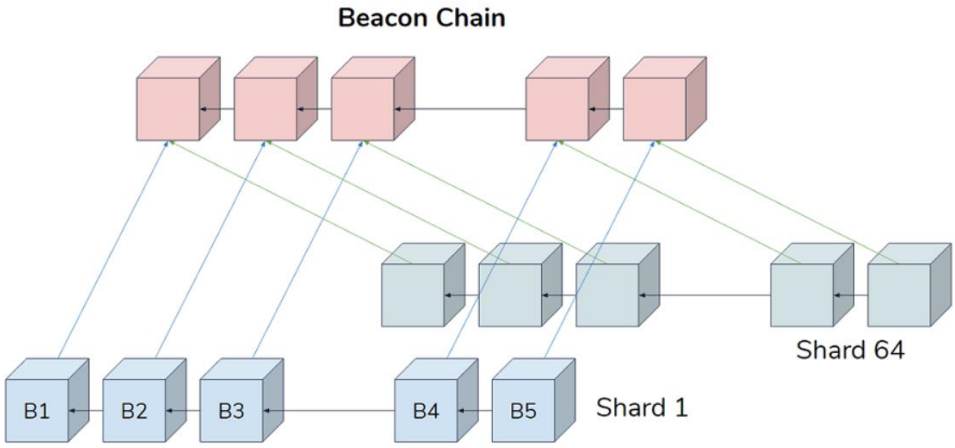


Figure 1-3-1 Ethereum 2.0 sharding[34]
*Beacon Chain in the figure will be the main chain of Ethereum 2.0.

[33] Ethereum.org Shard Chain https://ethereum.org/ja/upgrades/shard-chains/

[34] How Ethereum 2.0 Addresses the Problem of Rising Gas Prices and Scales Dai and DeFi https://blog.makerdao.com/eth2-0/

1-4-2 Blockchain Infrastructure Extension Service

The following is the overview and key technical characteristics of the following Layer 2 scaling solutions with the main objective of increasing throughput and reducing gas fees

Table 1-4-2: Technical Characteristics of the Service for Extending the Functionality of the Foundational Blockchain

Scaling Solution	Optimism	Arbitrum	Loopring	zkSync
Summary	- Developed by a startup born out of Ethereum's Plasma Group. - Compatible with Ethereum EVMs.	- Offchain Labs was founded and developed by researchers at Princeton University. - The company uses its own AVM (Arbitrum virtual Machine), which is compatible with EVM.	- Developed by Chinese startup Loopring. - It is the first zk-Rollup on the mainnet and is focused on building its own products and capabilities at layer 2.	- Developed by Matter Labs, a startup in Berlin. - Compatible with Ethereum EVMs.
Type of Rollup	Optimistic Rollup	Optimistic Rollup	zk-Rollup	zk-Rollup
Service Launch	2021	2021	2019	2020
Founder	Jinglan Wang, Karl Floersch, Kevin Ho (Plasma Group)	Steven Goldfeder (CEO), Edward W. Felten (Chief Science Officer), Harry Kalodner	Daniel Wang (Founder and CEO)	Alex Gluchowski (Co-Founder & CEO)
Development Language	Solidity	Solidity, Vyper, Yul	Solidity	Solidity, Zinc
Throughput	500TPS	500TPS	2,000TPS	2,000TPS
Major Stablecoins	USDT, USDC, DAI	USDT, USDC, DAI	USDT, USDC, DAI	USDT, USDC, DAI
Major DeFi	Uniswap, Maker, Aave	Uniswap, Maker, Aave	Loopring Exchange	Maker, SynFutures
Major NFT Services	Quixotic, Optipunks	STRATOS, tofuNFT	Gamestop	Tevaera, tofuNFT

Major Wallet	Metamask, Coinbase Wallet	Metamask, Coinbase Wallet	Loopring Wallet	Go Pocket, FoxWallet

1-4-3 Application Infrastructure and Applications

The technical characteristics of the following DeFi projects are described as below.

(1) Decentralized Exchange (DEX)

Table 1-4-3-1 Summary of major decentralized exchanges (DEXs)

DeFi Project	Uniswap	Curve Finance	SushiSwap
Establishment, Founder, Organization management	- Established in November 2018 - Founder: Hayden Adams - Organization management: Uniswap.org	- Established in August 2020 - Founder: Russian scientist Michael Egorov - Mr. Egorov holds 71% of CRV (Governance Tokens) - Organization management: Curve DAO	- Established in September 2020 - Founder: Chef Nomi, Co-Founder: 0xMaki (both pseudonyms) - In September 2020, management authority was transferred to Sam Bankman-Fried, CEO of Alameda Research. - Organization management: Sushiswap core team
Available blockchain	Ethereum Polygon Optimism Arbitrum	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum, etc.	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum, etc.
Outline, Features, etc.	- Protocol for token exchange of crypto-assets, stablecoins, etc. - Automated Market Maker (AMM) automatically determines the token exchange price. - Liquidity providers earn a fee for providing liquidity of any token pair to the liquidity pool.	- Decentralized exchange specializing in the exchange of stablecoins. - It is said to be possible to trade between stablecoins with low slippage rates and transaction fees.	- Created as a fork of Uniswap in September 2020. - Liquidity providers can be rewarded with SUSHI tokens (governance token) for providing liquidity.
TVL (as of 4/20/2022)	$7.04B	$10.32B	$1.49B

Governance	- Voting by UNI - Approved by 2 votes - Snapshot Voting (Selection of Proposal Targets) - Governance Voting (to approve or disapprove implementation)	- Voting by CRV - Approved by 2 votes - Snapshot Voting (Selection of Proposal Targets) - Governance Voting (to approve or disapprove implementation)	- Voting by SUSHI (Vote only once.) - Communities can veto at 40% of all issued governance tokens. - Some (considered small changes) are not voted on, but decided by the management and the core team.
Incidents	- 9/25/2020 When the $275 million was leaked in the attack on the exchange KuCoin, it was exchanged for ETH on Uniswap and allegedly laundered. - 4/18/2020 ERC-777 Reentrancy Vulnerability (see 2-2-4) attack results in $300,000 loss	- 11/11/2021 Governance attack (hijacking of votes through large purchases of governance tokens) resulting in $30 million in losses	- 9/17/2021 Supply chain attack (incorporating malicious code into the source) of the MISO platform (SushiSwap's platform for IDOs (fundraising by launching new tokens on the DEX)) resulted in a $3 million outflow

(2) Stablecoin Issuance Platform

In this report, the discussion is based on the following two categories of stablecoins

- Digital money type stablecoins: Tether, USD Coin, etc.

  Issued at a price pegged to the value of a fiat currency (e.g., 1 coin = $1) and redeemed at an amount equal to the issue price (and those equivalent thereto)

- Crypto-asset type stablecoins: DAI, TerraUSD, etc.

  Some, like DAI, attempt to stabilize value by holding other crypto-assets and stablecoins as overcollateral, while others, like TerraUSD, are unsecured and attempt to stabilize value algorithmically.

Table 1-4-3-2 Overview of Major Stablecoin Issuance Platforms

DeFi Project	Maker (DAI)	Tether (USDT)	USD Coin (USDC)	TerraUSD (UST)
Stablecoin Type	Crypto-asset type	Digital money type	Digital money type	Crypto-asset type
Establishment, Founder, Organization management	- Established in December 2017 - Founder: Rune Christensen (Danish) - Organization management: In order to increase the degree of decentralization as a decentralized autonomous organization, the MakerDAO took over operations of the Maker Foundation in July 2021.	- Established in 2014 - Issued and managed by Tether Limited, a Hong Kong limited company - iFinex (Hong Kong) manages Tether and exchange Bitfinex	- Established in September 2018 - Issued and managed by the Centre Consortium, founded by Circle and Coinbase	- Established in January 2018 - Founder: Do Kwon (CEO: Founder of TMON, Korea), Daniel Shin - Organization management: Terraform Labs (a subsidiary of Terra alliance) operates Seoul, Korea.
Available Blockchains	Ethereum Polygon Avalanche BNB Smart Chain	Ethereum Polygon Avalanche	Ethereum Polygon Avalanche BNB Smart Chain	Terra Ethereum Polygon Avalanche

	Optimism Arbitrum Loopring zkSync, etc.	BNB Smart ChainPolkadot Optimism Arbitrum Loopring zkSync, etc.	Polkadot Optimism Arbitrum Loopring zkSync, etc.	BNB Smart Chain Polkadot, etc.
Outline, Features, etc.	- When a new DAI is issued, the price is stabilized by depositing crypto-assets as collaterals above the DAI issue amount.	- It is believed that Tether owns and manages backing assets equivalent to the amount of the USDT issuance.	- It is believed that Circle owns and manages backing assets equivalent to the amount of USDC issuance.	- Algorithmically control the UST to maintain 1USD by adding/removing LUNA (native token of Terra blockchain). - Deposit USTs with Anchor Protocol and earn up to 19.5% yield
Issue balance [35] (as of 5/18/2022)	$6.52B	$79.71B	$52.26B	$11.28B
Governance	- Voting by MKR - Approved by Governance Poll (governance changes) or Executive Vote (technical changes)	- Operated and managed by Tether Limited	- Operated and managed by the Centre Consortium	- Voting with LUNA tokens - Vote only once. Decided by more than 50% of agrrements by the governance vote
Incidents	- 3/12/2020 The sharp drop in market prices prevented mandatory liquidation from catching up, and zero bids for collateral auctions resulted in a loss of $8.32 million (see 2-3-4).	- 3/1/2021 Ransom attack demanding 500 BTC via forged documents and threatening emails (no damage)	-	- 5/10/2022 A mounting commotion occurred as the market price fell due to the large volume of UST sales and the inability to maintain 1USD. Prices fell 87%.

[35] Cryptocurrencies https://coinmarketcap.com/coins/

(3) Lending Platforms

Table 1-4-3-3 Summary of Major Lending Platforms

DeFi Project	Aave	Compound
Establishment, Founder, Organization management	- Established in November 2017 - Founder: a serial entrepreneur Stani Kulechov - Organization management: Aavenomics community	- Established in 2017 - Founders: Robert Leshner, Geoffrey Hayes (CEO and CTO of Compound Labs, Inc, software developer of the Compound protocol) - Organization management: The Compound team is not considered to be involved in the operation.
Available Blockchain	Ethereum Polygon Avalanche BNB Smart Chain Optimism Arbitrum zkSync, etc.	Ethereum Avalanche BNB Smart Chain
Outline, Features, etc.	- Lenders can earn a yield by providing crypto-assets, stablecoins, or other tokens to the liquidity pool - Interest rates are automatically adjusted based on supply and demand. - Flash Loan (a transaction that is completed from borrowing to repayment within a single transaction) can be executed.	- Lenders can earn a yield by providing crypto-assets, stablecoins, or other tokens to the liquidity pool - Interest rates are automatically adjusted based on supply and demand.
TVL (as of 4/20/2022)	$11.46B	$6.34B
Governance	- Voting by AAVE - Approved by 2 votes 1) Snapshot voting (selection of proposal targets) 2) Governance Voting (decision on whether to implement)	- Voting by COMP - Vote only once. - Minimum 7 days from proposal of voting to its execution - Ability to disable a set of services in case of unexpected vulnerabilities
Incidents	-	- 10/4/2021 162 million in losses due to faulty upgrades - 9/30/2021 Upgrade Failure Leads to $90 Million in incorrect payments

(4) Derivatives platform

Table 1-4-3-4 Summary of major derivatives platforms

DeFi Project	Synthetix	Opyn.	Ribbon Finance
Establishment, Founder, Organization management	- Established in September 2017 - Founder: Australian Kain Warwick - Organization management: 5 DAOs ➢ Spartan Council ➢ Protocol DAO ➢ Synthetix DAO ➢ Ambassadors DAO ➢ GrantsDAO	- Established in 2019 - Founder: Zubin Koticha, Alexis Gauba, Aparna Krishnan - Organization management: team of three founders and partners	- Established in February 2021 - Founder. - Julian Koh - (Former Coinbase engineer) - Organization management: Ribbon DAO
Available blockchain	Ethereum Polygon Avalanche BNB Smart Chain	Ethereum	Ethereum
Outline, Features, etc.	- Allows users to generate and trade tokens (synthetic assets) linked to the price of fiat currencies, stocks, and commodities such as gold and oil. - Synthetic Assets are traded on a dedicated exchange called Synthetix Exchange (Kwenta).	- DeFi protocol that allows users to buy, sell, and create options - Allows users to exchange option spreads and combos, execute flash mint[36] (borrowing unsecured options up to repayment within one transaction), and automatically execute and create new options at maturity.	- DeFi's various derivatives can be combined to create any structured product - Packaged financial products that use a combination of derivatives to achieve specific risk/return objectives, such as betting on price volatility, increasing yield, or securing principal
TVL (as of 4/20/2022)	$276.1M	$111.4M	$106.8M
Governance	- The Governing Body approves the two improvement proposals. 1) Improvement proposal (SIP) Spartan Council interviews and approves SIP author	- Core team manages operations ➢ Whitelist/Blacklist registration ➢ Module Update ➢ Oracle Management ➢ Emergency system shutdown	- Voting with RBN tokens - Vote only once. - Snapshot Voting - Judged by 50% or more in favor or against

[36] What is a flash mint? https://github.com/opynfinance/v2-documentation

	2) Configuration Change Proposal (SCCP) Includes system existing parameter changes, otherwise same as SIP	➢ Withdraw excess token balance	
Incidents	- 6/25/2019 Oracle Attack on FX Price Feeds Loses $1 Billion	-	- 10/8/2021 Airdrop (benefit) attack converted $2.5 million after outflow

(5) Insurance

Table 1-4-3-5 Summary of major insurance platforms

DeFi Project	Armor	Nexus Mutual
Establishment, Founder, Organization management	- Established in November 2020 - Founder: Jose Macedo, - Azeem Ahmed, Robert Forster - Organization management: ArmorDAO Community	- Established in May 2019 - Founder: Hugh Karp, - Insurance Actuaries in the UK - Organization management: Nexus Mutual Community
Available blockchain	Ethereum	Ethereum Solana.
Outline, Features, etc.	- Protect your investment from the risks of smart contracts in common protocols such as Uniswap, Maker, AAVE, etc. - Detects changes in balances on supported protocols and prompts you to adjust your plan accordingly. The exact amount protected by each protocol is billed in seconds. - Based on Nexus Mutual's insurance, multiple protocols, coverage, etc. added.	- Decentralized insurance platform that allows risk sharing for smart contract vulnerabilities and other unforeseen events - The company provides decentralized insurance to users on the blockchain using ETH. A digital cooperative operating as a voluntary mutual in the UK, providing an "insurance alternative" to Ethereum users[37] - Drawing experience from prominent advisors and partners such as Kenetic, Blockchain Capital, Version One, Semantic Ventures, Collider Ventures, and others
TVL (as of 2022/4/20)	$511.5M[38]	$481.7M
Governance	- Voting with ARMOR tokens - Vote only once. - Hybrid control by two owners 1) Team multisig.	- Voting with NXM tokens - One screening and two voting 1) Decision making of Compensation by Advisory Board (White List)

[37] https://medium.com/multi-io/defi-explained-nexus-mutual-12d01f4471bb

[38] https://www.stelareum.io/en/defi-tvl/protocol/armor.html

	Managed by the management team 2) Governance Voting User Voting	- 2) Advisory Committee Vote - 3) Member Voting
Incidents	- 2/28/2021 Loss of $850,000 due to a fraud by the team member	- 12/4/2020 Targeted attack on founder's personal address results in $8 million loss

※ KYC / AML Requirements for Nexus Mutual

To become a member, you must verify your identity using the KYC / AML process. If this fails, the membership fee will be refunded

<Countries not eligible for membership>

China, Mexico, Syria, Ethiopia, North Korea, Trinidad and Tobago, India, Russia, and Tunisia, Iran, Serbia, Vanuatu, Iraq, South Korea, Yemen, Japan, Sri Lanka

(6) NFT (Non-Fungible Token Non-Fungible Token)

NFTs are generally unique, irreplaceable tokens within a smart contract that are recorded on the blockchain, and are utilized for services such as associating easily replicable items such as images, video, audio, and other types of digital files as metadata.

Table 1-4-3-6 Summary of main NFT services

DeFi Project	Opensea	CryptoPunks
Establishment, Founder, Organization management	- Established in December 2017 - Foundar: Co-founders Devin Finzer (CEO), Alex Atallah, CTO - Organization management: Opensea	- Established in June 2017 - Founder: Co-founders Matt Hall, John Watkinson - Organization management: Larva Labs
Available blockchain	Ethereum Polygon, etc.	Ethereum Polygon
Outline, Features, etc.	- NFT's largest project - The world's largest NFT marketplace - Based in New York, U.S.A.	- One of NFT's oldest projects - The First NFT art with ownership of each piece of art recorded in Ethereum - Purchased by Visa, a major credit card company, and is attracting attention.
Aggregate transaction value[39] (as of 2022/4/20)	$23.5B	$2.66B
Governance	Operated and managed by Opensea	Operated and managed by Larva Labs
Incidents	- 10/14/2021 Emergency fix for security vulnerability identified (measures completed in 1 hour, no damage)	-

[39] NFT Marketplaces https://dappradar.com/nft/marketplaces

1-4-4 Aggregation

Table 1-4-4 Summary of DeFi Aggregators

DeFi Project	Instadapp	DeFi Saver	1inch
Establishment, Founder, Organization management	- Established in December 2018 - Founder: Sowmay Jain (Co-founder & CEO) - Organization management: Instadapp Community	- Established in April 2019 - Founder: Nenad Palinkasevic - (Co-founder) - Organization management: Defi Saver	- Established in December 2020 - Co-founders: Sergej Kunz, Anton Bukov - Organization management: 1inch DAO
Available Blockchain	Ethereum	Ethereum	Ethereum Avalanche BNB Smart Chain, etc.
Outline, Features, etc.	- A smart wallet that aggregates DeFi protocols such as MakerDAO, Compound, and Uniswap for managing assets. - The dashboard allows users to see all DeFi in one place.	- One-stop management application for DeFi protocol. - Unique automated asset management and liquidation protection features. - Known as a leverage management tool.	- Liquidity protocols provide decentralized token swaps as automated market makers (AMMs) - The protocol is designed to capture the marginal gains of arbitrage.
TVL (as of 4/20/2020)	$5.19B	$509.7M	$14.5M
Governance	- Voting with INST tokens - Snapshot (selection of proposal targets) - Governance Vote (decision to implement or not)	Managed and operated by Defi Saver	- Voting with 1INCH tokens - Snapshot (selection of proposal targets) - Governance Vote (decision to implement or not)
Incidents	-	- 10/8/2020 Loss of 310,000 DAI due to vulnerability in token exchange contract	-

1-4-5 User and User Interface

(1) User Interface

When users use DeFi's functions and services, such as crypto-asset purchases and exchanges and crypto-asset deposits into the liquidity pool, they operate transactions from the user authentication screen or user operation screen (GUI: Graphical User Interface) of a web browser or smartphone application.

(2) Operators (including administrators and authorized persons who deploy)

DeFi system operation tasks, such as deployment and maintenance of smart contracts and monitoring of DeFi protocol operation, are controlled from the user operation screen of the client software.

(3) DeFi system developer

Develop and test DeFi protocols (smart contracts) using development tools such as Truffle.

(4) Code auditors

Auditing of smart contracts through auditing tools and test execution.

(5) Community participants

Posting opinions and proposals on the DeFi project community forum and on-chain voting with governance tokens.

1-5 Interoperability Analysis

Interoperability between DeFi projects deployed on the same blockchain as well as interoperability between Ethereum blockchain and Layer 2 scaling solutions and main and side chains were analyzed to examine their technical characteristics and challenges.

(1) Token interoperation between DeFi projects within the blockchain (Ethereum)

Ethereum has developed token standards such as ERC-20, and many DeFi projects are issuing governance tokens and stablecoins in compliance with these token standards. The tokens that comply with the standard can be used as the same type of operating target in any DeFi project. A token that conforms to the standard can be used in any DeFi project as an operating target of the same type. Therefore, interoperability is high.

However, it also means that any DeFi project could be linked to the project, so there is a risk of unexpected attacks in transactions such as arbitrage.

(2) Interoperation between Ethereum mainchain and Layer 2 solutions

The use of Layer 2 solutions is growing as a scaling measure for Ethereum, and many DeFi projects are adopting Layer 2 solutions. Layer 2 solutions are EVM compatible, and the same development languages and libraries as Ethereum work. On the other hand, it is still a developing technology, and there are issues such as the fact that validity is not verified at the time data is written and transactions must wait for the fraud proof challenge period (e.g., Optimistic Rollup) to be confirmed.

(3) Interoperation between Ethereum main chain and side chains

The Ethereum mainchain and sidechains are provided with the ability to connect via a two-way bridge, and many sidechains are operating in connection with Ethereum. Many sidechains are EVM-compatible and function with the same programming language and libraries as Ethereum. In addition, when funds are exchanged between the main chain and sidechains, it is possible to lock funds into a two-way bridge and exchange funds, preventing double payments.

In recent years, Ethereum transaction congestion and rising gas fees have led to increased use of sidechains in search of faster processing and lower gas fees for gaming and other activities. At the same time, there is a growing risk that billions of dollars of large sums of money are locked up in two-way bridges and targeted by attackers, and there have been a number of incidents, as discussed below.

Chapter 2. Analysis of Major DeFi Projects

This chapter identifies issues, problems, and risk matters by selecting major DeFi projects and conducting a detailed study of their organization, stakeholders, technical characteristics, governance operations, collaboration with financial institutions, and incident cases.

This chapter is organized as follows: in 2-1, we select the DeFi projects to be studied from three services: decentralized exchanges, stablecoin issuance, and lending; in 2-2 to 2-4, we report the results of a detailed study of the three selected DeFi projects; in 2-5, we compare the results of the analysis of the three DeFi projects to identify overall trends and the characteristics of each DeFi project; and in 2-6, we examine incident cases that occurred in other DeFi projects and analyze risk matters. Finally, in 2-7, the results of the analysis of trust points in the chain of trust is explained.

2-1 Identification of DeFi projects to be studied

With reference to indicators such as TVL and survey objectives, the following three services were selected as targets from the six main DeFi projects mentioned above.

(1) Decentralized Exchange (DEX)

This is a basic use case for DeFi, which automatically exchanges multiple crypto-assets/stablecoins, and therefore should be included in the study.

(2) Crypto-asset-based stablecoin issuance platform

Among DeFi projects that issue stablecoins, which are often used in crypto-asset and DeFi transactions, crypto-asset-type stablecoins, whose issuance itself is also decentralized, should be the object of the study.

(3) Lending Platforms

Since this is a basic use case of DeFi and TVL is the largest, it is the subject of the study.

2-1-1 Selection of DeFi Projects to be Investigated (Decentralized Exchange)

Regarding decentralized exchanges, based on the comparison of the following DeFi projects, Uniswap is selected for investigation. Because of its large TVL, incident cases, and technical characteristics that should be investigated, such as making smart contracts non-upgradeable, it was determined that Uniswap was appropriate.

Table 2-1-1 Selection of DeFi Projects to be Investigated (Decentralized Exchange)

DeFi Project	Uniswap	Curve Finance	SushiSwap
Modification of existing smart contracts (Addition of products and services, change of parameters, etc.)	- Only some of the parameters can be modified	- Modified by Curve team after passage of governance vote	- After passing a governance vote, determined by a vote of 9 community members
Modification of existing smart contracts (modification of core contract)	- Core contract is not upgradeable	- Modified by Curve team after passage of governance vote	- After passing a governance vote, determined by a vote of 9 community members

Deployment of new smart contracts (e.g., deploying new smart contracts for version upgrades, etc.)	- Conducted by the development company (Uniswap Labs)	- Conducted by the Curve team	- After passing a governance vote, determined by a vote of 9 community members
Emergency activation (e.g., emergency suspension of service)	- Core contract cannot be stopped.	- Determined by a vote of 9 community members.	- Determined by a vote of 9 community members.
Governance Token	UNI	CRV	SUSHI
Number of addresses holding governance tokens and percentage of addresses holding such tokens	- 276,000 addresses - Percentage of 1st place holdings: 17.34% - Percentage of top 10 addresses held 53.42%	- 52,000 addresses - Percentage of 1st place holdings: 36.07% - Percentage of top 10 addresses held 83.60%	- 17,000 addresses - Percentage of 1st place holdings: 18.19% - Percentage of top 10 addresses held 65.18%
Governance Vote Proposed Subject	- Add or change liquidity pools - Change numerical parameters such as commissions - Proposed items are not limited, but the core contract is unchangeable and the topics related to other technical characteristics will be limited as the scope of the governance vote.	- Add or change liquidity pools - Change numerical parameters such as commissions - Core contract modification	- Core contract changes and use of funds
Proposal approval conditions	1) Snapshot: - Select proposal targets by soliciting a wide range of opinions - Quorum 50,000 UNI (0.05% of total), majority of votes cast in favor 2) Governance Vote: - Quorum of 40 million UNI (4% of the total) to decide whether or not to implement the proposal; majority of the votes cast are in favor.	1) Snapshot: - Quorum 30%, 51% in favor 2) Governance Vote: - Quorum 15%, 60% in favor.	1) Snapshot: - A quorum of 5 million SUSHI tokens and a majority of the votes cast are in favor. 2) Governance Vote: - Decided by a multisig of 9 community members after being passed by vote (6 of 9)

Number of votes (as of 12/12/2021)	1) 7 of 32 cases passed Approval rate 22% 2) 5 out of 6 approved 83% approval rate	1) 60 of 68 approved Approval rate 88a% 2) All 14 cases passed 100% approval rate	13 of 15 cases passed 87% approval rate

2-1-2 Selection of DeFi Projects to be Investigated (Crypto-asset Stablecoin Issuance Platform)

For the crypto-asset stablecoin issuance platform, Maker is selected for investigation based on the following DeFi project comparison results: the TVL is expensive, the transition to a decentralized autonomous organization (DAO) is the most advanced case among the DeFi projects, and the other DeFi projects are all centralized organizations run by companies, and Maker fits the purpose of investigating a diverse set of subjects, it was deemed appropriate as a research target.

Table 2-1-2 Selection of DeFi Projects to be Investigated (Stablecoin Issuance)

DeFi Project	Maker (DAI)	Tether (USDT)	USD Coin (USDC)
Modify existing smart contracts (add products, services, change parameters, etc.)	- Voted on by Governance Tokens	- Implemented by Tether Limited	- Implemented by Centre Consortium
Modification of existing smart contracts (modification of core contract)	- Voted on by Governance Tokens	- Implemented by Tether Limited	- Implemented by Centre Consortium
Deployment of new smart contracts (e.g., deploying new smart contracts for version upgrades, etc.)	- Voted on by Governance Tokens	- Implemented by Tether Limited	- Implemented by Centre Consortium
Emergency activation (e.g., emergency suspension of service)	- Decision by off-chain voting: executed at 50,000 MKR (5% of total)	- Implemented by Tether Limited	- Implemented by Centre Consortium
Governance Token	MKR	-	-
Number of addresses holding governance tokens and its percentage	- 76,000 addresses - Percentage of 1st place holdings: 17.39% - Percentage of top 10 addresses held 45.38%	-	-
Governance Vote Proposed Subject	Two types of proposals will be made depending on the nature of the proposal 1) Governance Poll - Stabilization fees, collateral ratio changes, etc. 2) Executive vote - Technical changes to the Maker protocol	-	-

Conditions for passage of a voting	- Same conditions for both 1) and 2) - Quorum of 10,000 MKR (1%), majority is in favor	-	-
Number of votes (as of 12/12/2021)	1) Approved 271 out of 302 cases, 90% approval rate 2) Approved 47 out of 48 cases, 98% approval rate	-	-

2-1-3 Selection of DeFi projects for study (lending platform)

Regarding lending platforms, based on the comparison of the following DeFi projects, Aave is selected for the study because of its large TVL and its services rarely seen elsewhere, such as the launch of KYC services for institutional investors.

Table 2-1-3 Selection of DeFi Projects for Investigation (Lending)

DeFi Project	Aave	Compound
Modification of existing smart contracts Addition of products and services, parameter changes, etc.	- Voting by Governance Token	- Voting by Governance Token
Modification of existing smart contracts (modification of core contract)	- Voting by Governance Token	- Voting by Governance Token
Deployment of new smart contracts (e.g., deploying new smart contracts for version upgrades, etc.)	- Aave Core Team determines	- Compound Labs determines
Emergency activation (e.g., emergency suspension of service)	- Aave Core Team determines	- Determined by a multisig of 6 community members (4-of-6)
Governance Token	AAVE	COMP
Number of addresses holding governance tokens and its percentage	- 100,000 addresses - Percentage of 1st place holdings: 18.54% - Percentage of top 10 addresses held 62.30%	- 181,000 addresses - 1st place retention rate: 28.99% - Percentage of top 10 addresses held 54.32%
Conditions for passage of a voting	Two types of proposals will be made depending on the nature of the proposal 1) Short-time lock execution - Some changes requiring quick intervention, etc. 2) Long time lock execution - Changes affecting governance	- Cast an on-chain voting (one time only)
Proposal approval conditions	1) Short-time lock execution - Quorum of 2% and difference in favor/against is 0.5% or more	- Proposal: 65,000 COMPs (0.65% of the total) in favor

	2) Long-time lock execution - Quorum of 20% and a difference in favor/against is 15% or more	- Pass: 400,000 COMP (4% of the total) and a majority of the votes cast
Number of votes (as of 12/12/2021)	- Approved 41 out of 50 cases, 82% approval rate	- Approved 32 out of 38 cases, 84% approval rate

2-2 Analysis of the decentralized exchange Uniswap

Uniswap is the subject of a detailed research study, including a project overview, governing body, key technical characteristics, governance operations, and incident cases. Uniswap has some unique fetures; a development company Uniswap Labs is considered to be involved to some extent in the management of the Uniswap community, as well as Uniswap is unique in that it makes smart contracts non-upgradeable. The investigation of each item clarifies the actual situation and identify risk issues.

2-2-1 Overall Project Overview

The main components of Uniswap, their mapping and community overview are shown in the figure and table below.

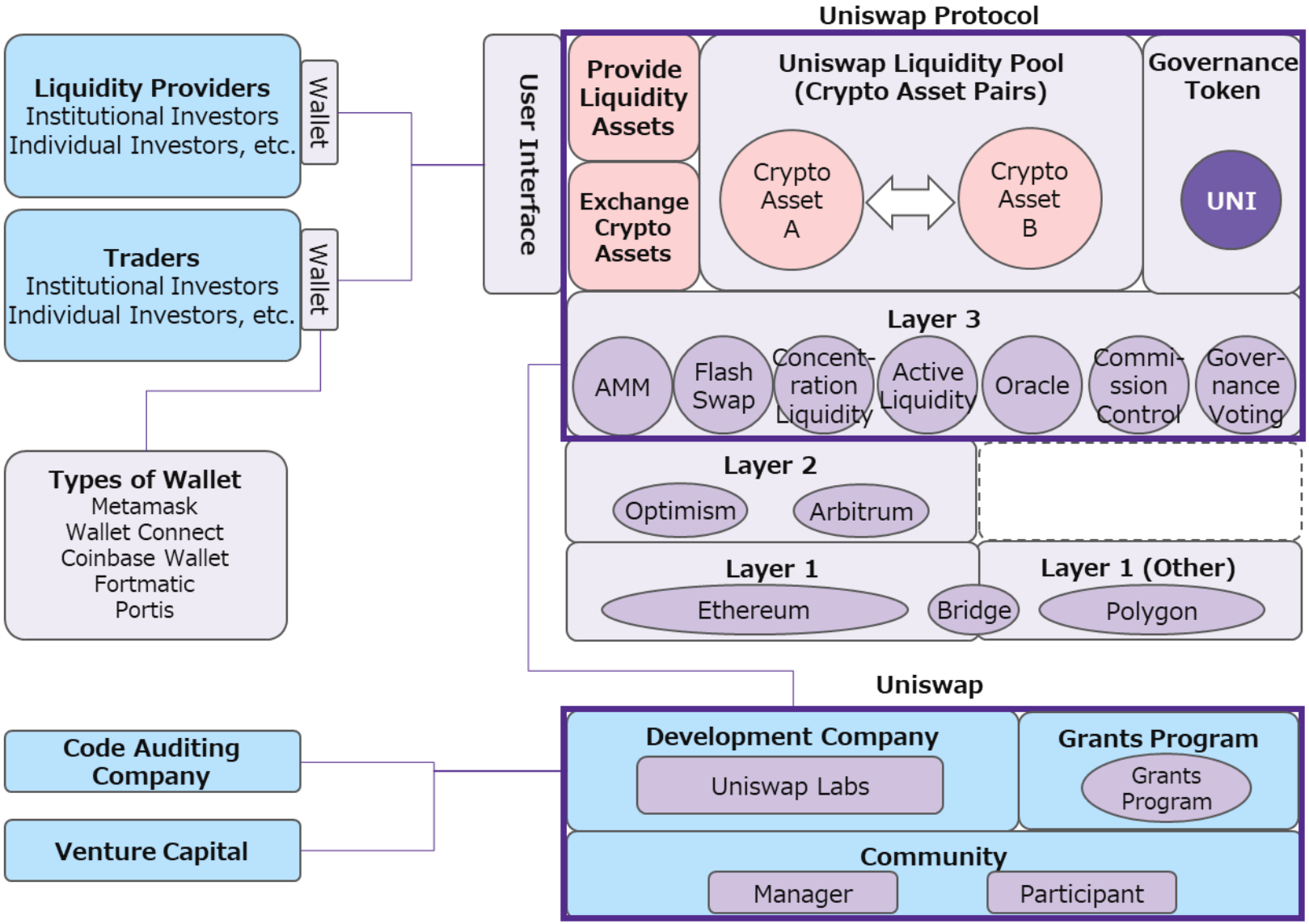


Figure 2-2-1-1 Main components of Uniswap

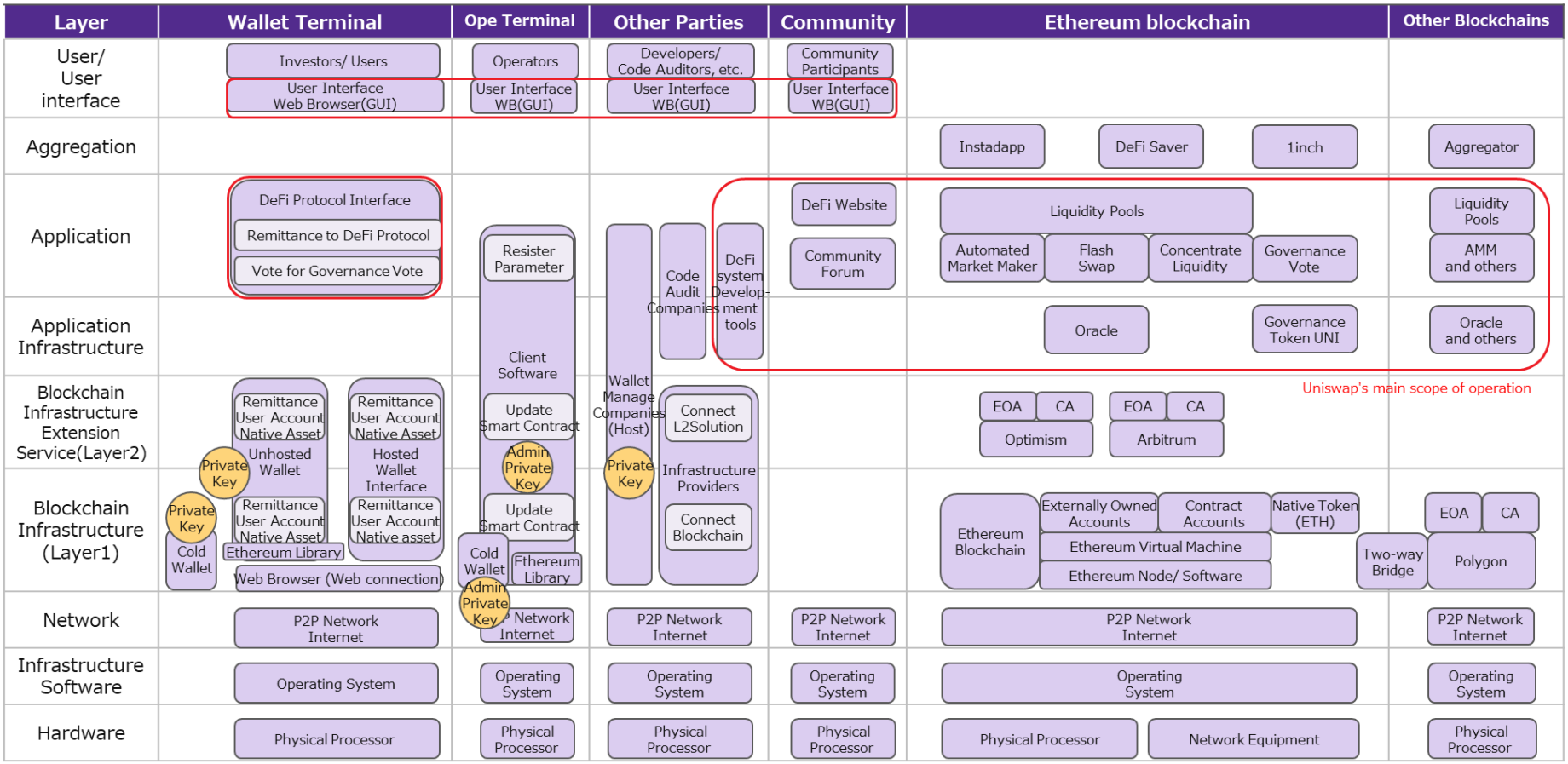


Figure 2-2-1-2 Mapping of main components of Uniswap

Table 2-2-1 Uniswap: Community, Development Company, and Version Trends

Classification	Item	Summary	Supplementary information
Organization	Community	Uniswap Community Operated by governor token holders (addresses held: 276,000)	Active under the name of DAO.
	Development company	- Uniswap Labs - Location: New York, United States - Founder, CEO: Hayden Adams - Date of fondation: Nov. 2018	- Development and management of Uniswap protocols and various tools - Operation of the website (Uniswap.org) - SEC (U.S. Securities and Exchange Commission) reportedly conducted an investigation into Uniswap Labs (Sep. 2021).[40]
Working Version	Uniswap Version and Main Functions	1) Uniswap v1 - Launched in November 2018 - Developed in Vyper language. Main Functions ➢ AMM (Automated Market Maker) ➢ Liquidity pooling (exchange of crypto-asset pairs) via ETH, etc.	- The three versions continue to operate separately. - Uniswap v1 (as of March 2022) - Tradable crypto-assets: approx. 200 - Trading Pairs: 385
		2) Uniswap v2 - Launched in May 2020 - Developed in Solidity language - Main Functions ➢ Liquidity pooling among crypto-assets (not via ETH) ➢ Flash SwapTWAP (time weighted average price) Oracle, etc.	- Uniswap v2 (as of March 2022) - Tradable crypto-assets: 1,909 - Trading pairs: 3,259
		3) Uniswap v3 - Launched in May 2021 - Developed in Solidity language - Main Functions ➢ Liquidity aggregation functions (e.g., concentrated liquidity) ➢ Extended commissions, (e.g., specification changes to NFT, 3 commission rates, etc.)	- Uniswap v3 (as of March 2022) - Tradable crypto-assets: 456 - Trading Pair: 915

[40] SEC Investigating Uniswap Labs: Report https://www.coindesk.com/policy/2021/09/03/sec-investigating-uniswap-labs-report/

		➢ Oracle Advancement, etc.	

2-2-2 Main Technological Characteristics

The main technological characteristics of Uniswap are outlined below.

(1) AMM (Automated Market Maker)[41]

- 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 since Uniswap v1).

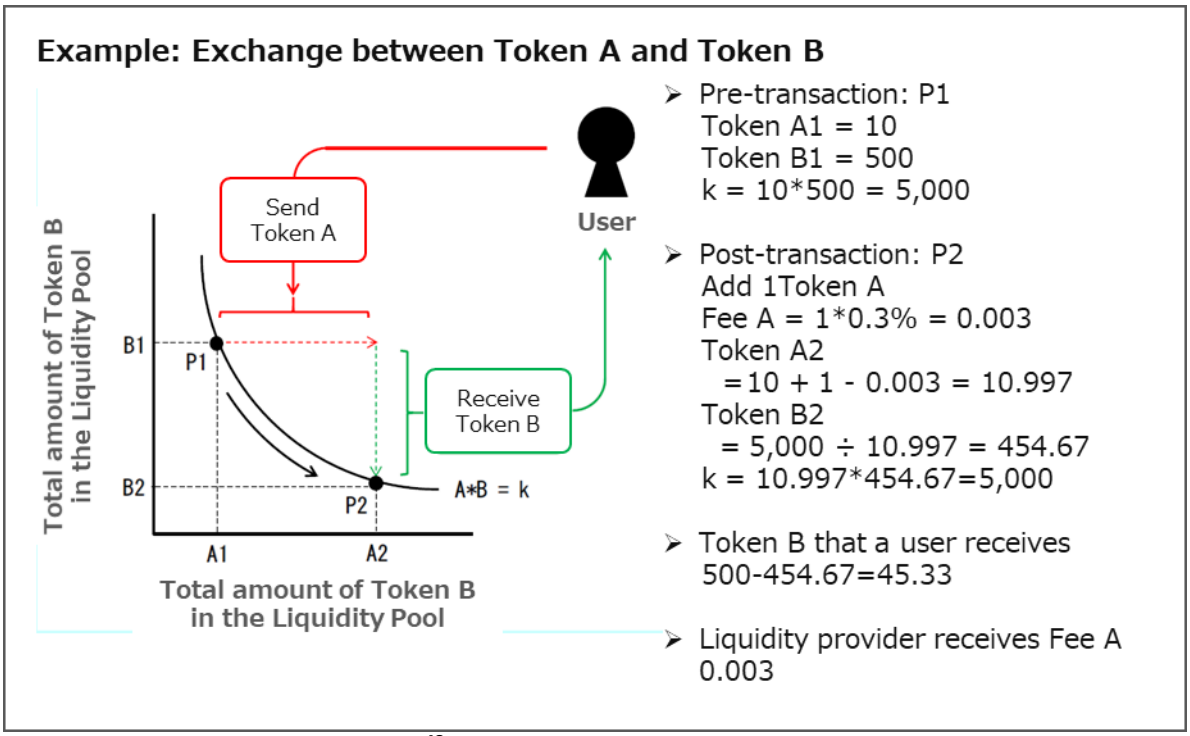


Figure 2-2-1 Uniswap AMM[42] (The Figure cited from Bank of Japan website)

(2) Flash Swap[43]

- 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

[41] What Is an Automated Market Maker? https://www.coindesk.com/learn/2021/08/20/what-is-an-automated-market-maker/

[42] Decentralized Finance in Crypto-assets The Emergence of Autonomous Financial Services and the Search for Governance https://www.boj.or.jp/research/wps_rev/rev_2021/data/rev21j03.pdf

[43] Uniswap v2 Docs Flash Swap https://docs.uniswap.org/protocol/V2/concepts/core-concepts/flash-swaps

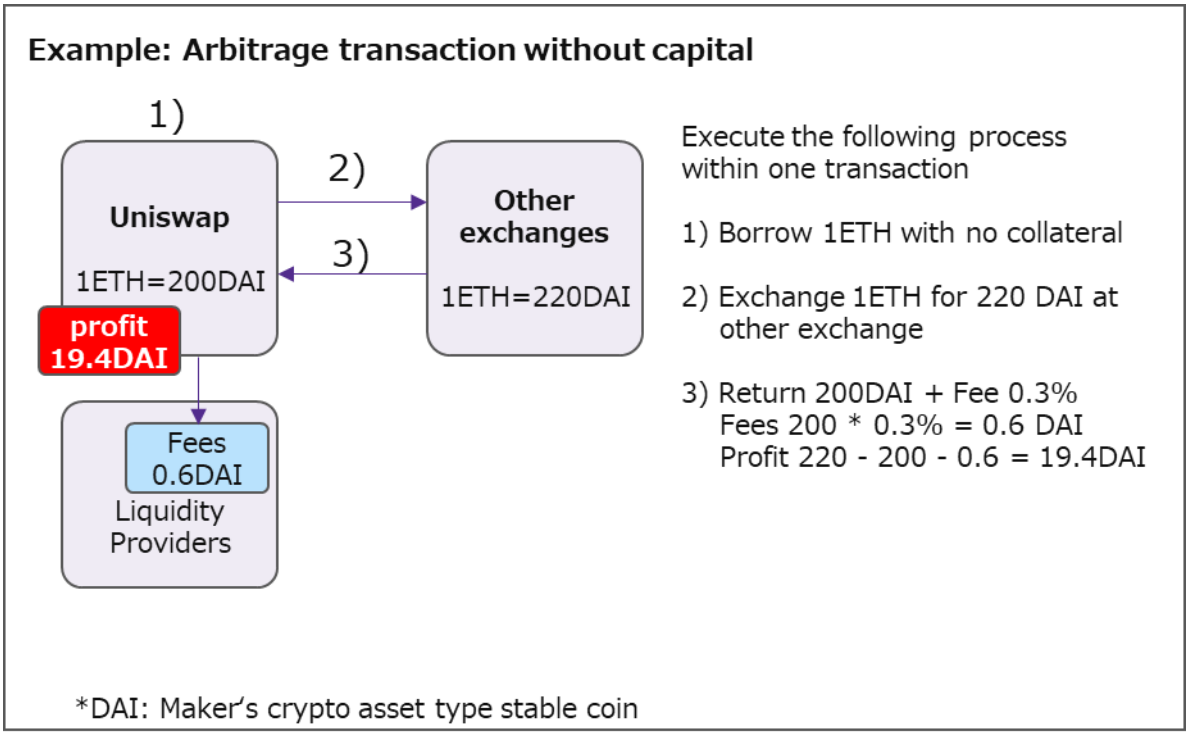


Figure 2-2-2 Uniswap: Flash Swap

(3) Concentrated Liquidity [44]

- 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.

[44] Introducing Uniswap v3 https://uniswap.org/blog/uniswap-v3

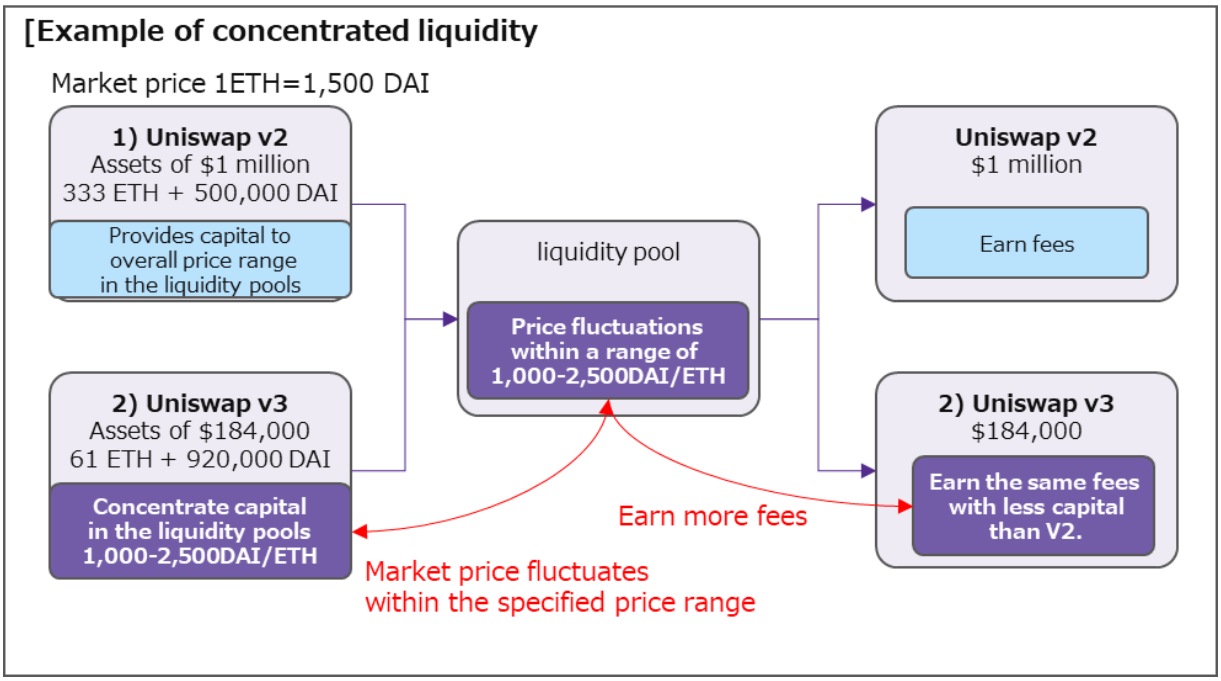


Figure 2-2-3 Uniswap: Concentrated Liquidity Function

<Description of figure 2-2-3>.

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.

(4) Flexible fees in v3[45]

- Multiple fee categories offered per liquidity pool and liquidity provider
  - ➢ Uniswap v1, v2 Fixed at 0.3% (hard coded)
  - ➢ Uniswap v3 Choose from 0.05%, 0.3%, or 1%.
- 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)
  - ➢ Uniswap v2: Governance vote enables governance token holders to earns 0.05% of 0.3% commission
  - ➢ Uniswap v3: Governance vote enables governance token holders to set between 10-25% of commission

[45] Uniswap v2 Overview https://uniswap.org/blog/uniswap-v2

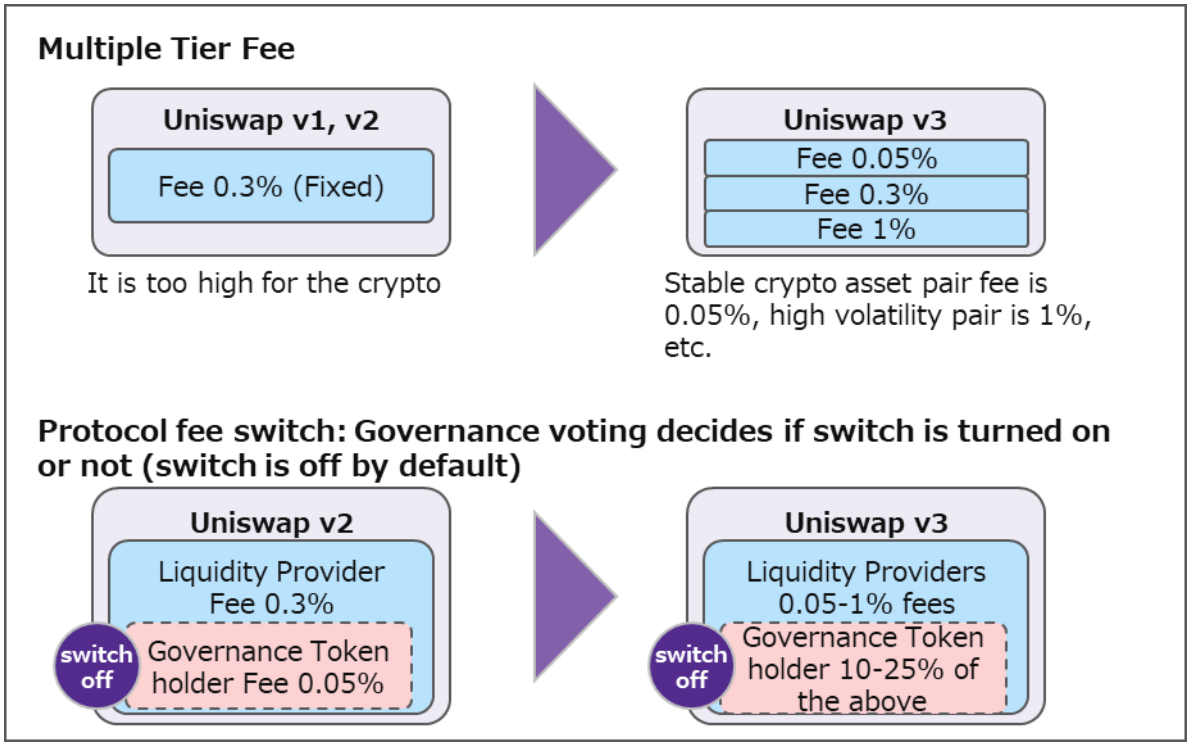


Figure 2-2-4 Flexibility of Uniswap Fees

(5) Advanced Oracles

- Uniswap v2[46] : TWAP (Time Weighted Average Price) Oracle
  - ➢ Measure the market price at the start of each block, calculate the cumulative price (Σ price x block generation time interval) 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[47] : TWAP efficiency improvement
  - ➢ Efficiently obtain TWAP within the past 9 days, contributing to lower gas costs

[46] Price Oracles https://uniswap.org/blog/uniswap-v2#price-oracles

[47] Advanced Oracles https://uniswap.org/blog/uniswap-v3

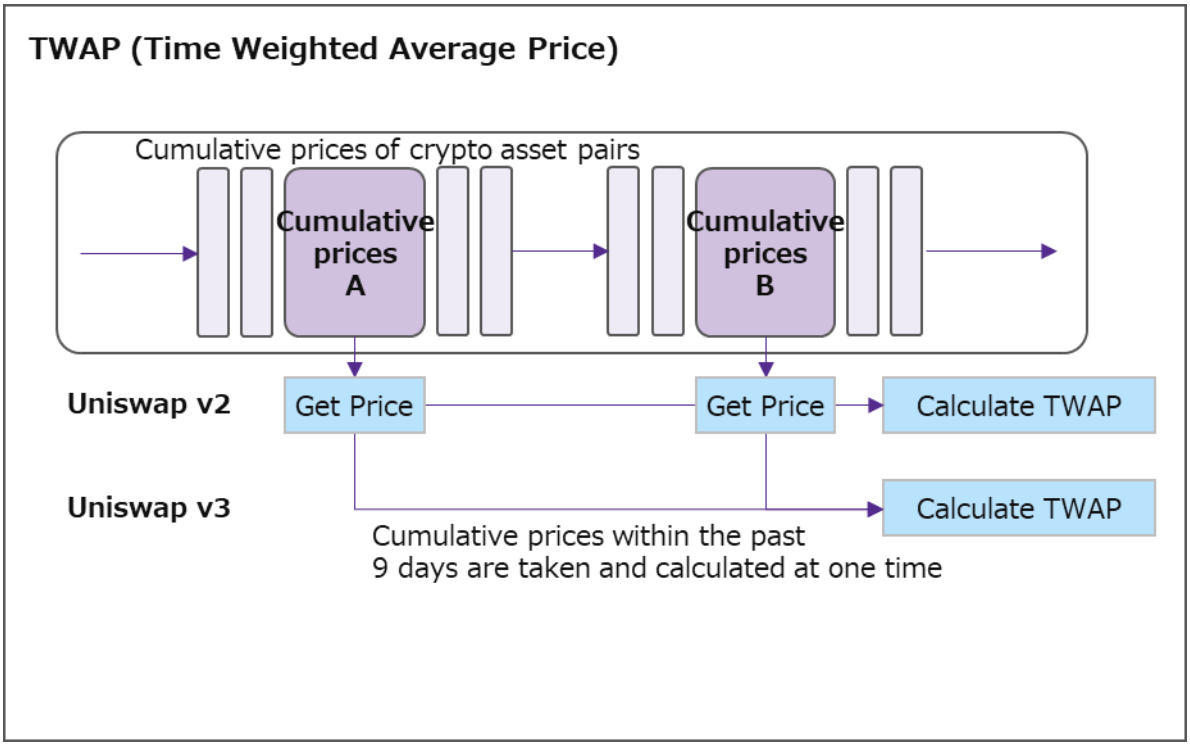


Figure 2-2-5 Uniswap Oracle

(6) Scaling

- Uniswap v3 is being deployed on Ethereum's Layer 2 solution as well as on non-Ethereum blockchains to address the issues of high gas fees and slow processing speeds caused by Ethereum's increasing number of transactions. Deployment.

Table 2-2-6 Uniswap Deployment Destination

Item	Summary	Supplementary information
Layer 2 solution	Optimism ➢ Uniswap v3 deployed shortly after Optimism service launch in July 2021	- Optimistic Rollup scaling technology can increase processing speed and reduce fees. - However, because of the waiting period until the transaction is fully guaranteed, a third-party liquidity provider must be used for immediate processing (fees will apply).
	Arbitrum ➢ Uniswap v3 deployed shortly after Arbitrum service launch in September 2021	- Arbitrum Rollup method is used, which utilizes Optimistic Rollup and their original Layer 2 solution “arbitrum one”
Blockchain	Ethereum Uniswap v1, v2, v3 Polygon Uniswap v3 - Polygon service launched in April 2019 - Uniswap v3 deployed in December 2021	- Provide scaling solutions using Polygon, Ethereum-compatible blockchain network

(7) Possibility to change (upgrade) smart contracts

Table 2-2-7 Uniswap: Smart Contract Upgradability

Item	Summary	Supplementary information
Possibility to change smart contracts	1) Core Contracts - Uniswap v1, v2 Core contract is not upgradeable by design - Uniswap v3 Core contract is not upgradeable by design (except for fee parameters)	- Core contract: Critical logic covered, minimal design Liquidity Pool, AMM, Flash Swap, Concentrated Liquidity, Advanced Oracles - 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 - Can be changed, added, or deleted without restriction (including fee changes)	- External contracts outside the core: fees, peripherals, interfaces, governance voting, etc. - Uniswap Labs to implement following passage of governance vote

(8) License management

Table 2-2-8 Uniswap: License Management

Item	Summary	Supplementary information
License protection for core contracts	Commercial license protection for Uniswap v3 protocol - 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. - Licensing periods can be changed or waived at any time through a governance vote. - Licensed includes Smart Contracts, Math Libraries, Peripheral Contracts, Interfaces, and Developer SDKs - Source code can be referenced. - 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.[48]	- Uniswap Labs, the developer, entrusted the license management authority of the source code to a governance token holder. - The case of not making it clear that it is not open source without making it reusable

2-2-3 Cooperation with Financial Institutions

Table 2-2-3 Uniswap: Cooperation with Financial Institutions

Item	Summary	Supplementary information

[48] https://www.coindesk.com/tech/2021/03/23/uniswap-v3-introduces-new-license-to-spoil-future-sushis/

Cooperation with Financial Institutions	Announced a tie-up with a Fintech company to explore market entry into the consumer finance domain.[49]	- PayPal, Robinhood (U.S. stock management app operator) - E*Trade (U.S. online brokerage firm) - Stripe (U.S. online payment), etc.
	Listed ETPs (exchange-traded products) passively linked to UNI[50] - Listed through Valour (Swiss Asset Management Company), a subsidiary of DeFi Technologies (Canadian Tech company)	- Frankfurt, Germany Stock market Euro-denominated Valour Uniswap ETP (October 2021) - Swedish Stock Market Krona Jian Valour Uniswap SEK (December 2021)
	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)	- Crypto-assets covered: AAVE, UNI, ANT, CRV, MKR, SNX, 1INCH
	Launch of custody and trading services (November 2021) - Commonwealth Bank (Australia) launches 10 crypto exchanges and custody services in partnership with Gemini Exchange and Chainalysis.	- Commonwealth Bank: Established in 1911 - Crypto-assets covered: BTC, ETH, BCH, UNI, LINK, MATIC, AAVE, COMP, LTC, FIL
	Offer trading and custody of DeFi related stocks (January 2022) - Arab Bank Switzerland (Switzerland) offers 10 different crypto-asset services.	- Arab Bank Switzerland: Established in 1962 - Crypto-assets covered: AAVE, FTM, COMP, SNX, LINK, MATIC, GRT, CRV, UNI, YFI

2-2-4 Governance operations

[49] https://www.coindesk.com/business/2021/07/28/uniswap-says-its-talking-with-paypal-robinhood-and-more-in-deleted-video/

[50] https://valour.com/press/valours-uniswap-exchange-traded-product-etp-goes-live-on-nordic-growth

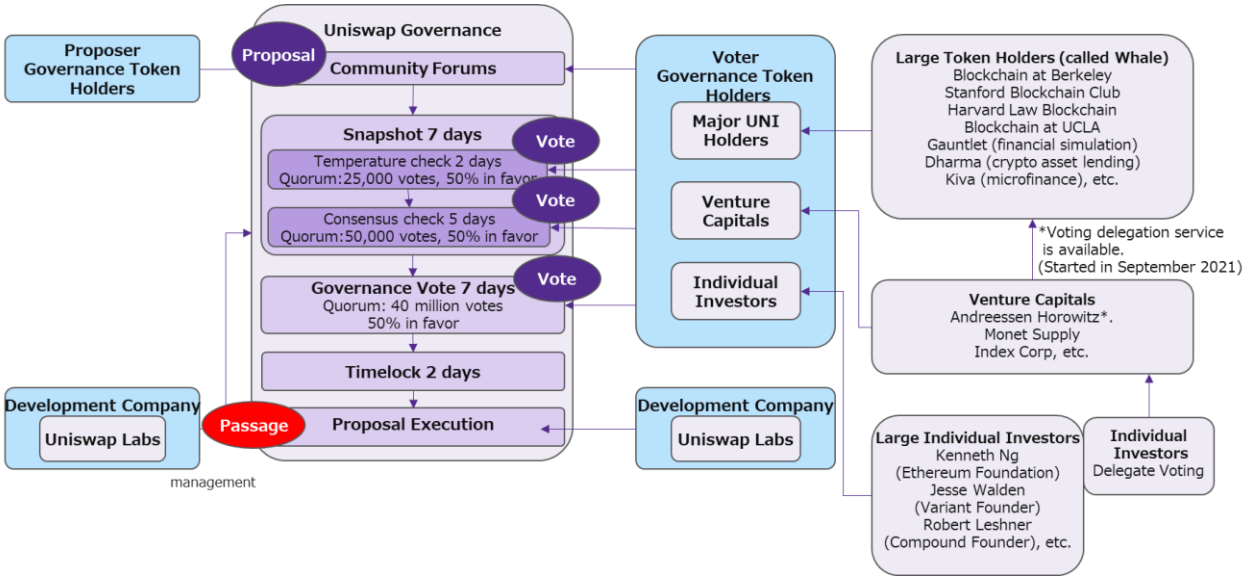


Figure 2-2-4 Governance Voting Process with UNI

(1) Community

Table 2-2-4-1 Uniswap: Community

Item	Summary
Purpose of the community (summarized from official documentation)[51]	- UNI (governance token) is introduced for the purpose of community-led growth, development, and self- sustainability, enabling shared community ownership and a vibrant, diverse, and dedicated governance system. - Uniswap has always embraced the tenets of neutrality and trust minimization: it is crucial that governance is constrained to where it is strictly necessary. - Uniswap governance framework is limited to contributing to both protocol development and usage as well as development of the broader Uniswap ecosystem.
community	- Decentralized Autonomous Organization (DAO) by the governance token UNI holders - No legal representatives, no management bodies such as board of directors or board of trustees, no auditors

(2) Governance tokens (UNI)

Table 2-2-4-2 Uniswap: Governance Token

Item	Summary	Supplementary information
Distribution of UNI	A total of 1 billion UNI will be distributed over 4 years starting in September 2020. - Community Members: 60.00% (600 million UNI) - Team members and employees: 21.266% (212.66 million UNI) - Investors: 18.044% (180.44 million UNI) - Advisors: 0.69% (6.9 million UNI)	- Already distributed about 500 million UNI (as of December 2021) - Undistributed tokens are locked to the smart contract

[51] Introducing UNI https://uniswap.org/blog/uni

Number of addresses held by UNI[52] (as of Jan. 2022)	- Number of addresses held by UNI: 276,000 - Percentage of 1st place holdings: 17.34% - Percentage of top 10 addresses held 53.42%	- The 5-7 addresses of major UNI holders (Whale) who are delegated to vote are the major decision makers (from Blog)[53] - A proposal to review the voting method and proposal thresholds were rejected.
UNI Features	- Voting rights in on-chain voting (governance tokens)	-

(3) Decision-making

Table 2-2-4-3 Uniswap: Decision Making

Item	Summary	Supplementary information
Decision-Making Methods[54]	Governance voting by UNI in the following two phases 1) Snapshot - Vote twice: temperature check and consensus check 2) Governance Vote - Decide whether to implement the proposal - Voting run for 7 days each in 1) and 2) and 2 days in TimeLock after passage.	- Snapshot voting is conducted off-chain and governance voting is conducted on-chain. - Temperature check: determine if there is sufficient will to change the status quo - Consensus check: Establish a formal discussion of the proposal
Conditions for passage of governance vote	1) 50,000 UNI (0.005% of total to be distributed) in favor 2) Proposal: 2.5 million UNIs (0.25% of total to be distributed) in favor To pass: Quorum 40 million UNI (4% of total to be distributed), majority of votes cast is in favor	- The possibility of manipulation of community opinion by large UNI holders or anonymous or pseudonymous persons who have temporarily purchased large quantities of UNI in the market, since the management of governance is entrusted to UNI holders.
Actual number of votes cast (2021)	1) 27 out of 35 approved (77% approval rate) 2) 6 out of 7 approved (86% approval rate)	- Fewer proposals were made than in other projects.
Items that can be proposed in the Governance Vote	1) Addition, modification, or deletion of external contracts other than core - Interfacing with other blockchains (e.g., new deployments) - Renewal of Governor Bravo* (contract for governance), etc.	- The core contract is non-upgradeable by design and cannot be modified or stopped. No countermeasures have been determined in the event when a vulnerability is discovered.

[52] Etherscan Token Uniswap https://etherscan.io/token/0x1f9840a85d5af5bf1d1762f925bdaddc4201f984

[53] https://gov.uniswap.org/t/consensus-check-abolish-delegates-and-change-the-uni-governance-voting-system/13458

[54] https://docs.uniswap.org/protocol/concepts/governance/process

	2) Addition, modification, and deletion of parameter values - Add/ delete liquidity pools - Change parameter values such as commissions - Change fee settings/ change protocol fee switce (on/off) - Allow UNI holders to collect a portion of liquidity provider fees (governance vote allows for fee collection), etc.	-
	3) Change in community management - Use of community funds (e.g., education funds) - Changes in governance operations (thresholds for governance proposals, review of voting methods)	- Large UNI holders can manipulate commission profits by voting, and there are no preventive measures. - If some UNI holders collude to take the majority, there is a concern that profits will be defrauded. However, if fraud is discovered, participants will leave and the market will shrink, which may result in a self-cleansing effect.
	4) Modification of the term of core contract commercial use prohibition license, waiver - v3 has a two-year ban on commercial use in the license, but the license control can be changed by a governance vote.	- A two-year license was introduced to prevent diversion to other projects, but a governance vote can allow this to be overturned.

※Governor Brabo:

- Smart contract for governance developed by Compound and deployed at Uniswap
- Adopted by governance vote.

<Features>

- Upgradeable smart contracts in Governor Brabo itself
- Add "Abstain" option for voting
- Added the ability to add comments when voting
- Ability to change voting parameters (voting period, extension of voting body, quorum thresholds)
- Proposer can cancel his/her proposal
- Delete Guardian (Governance Manager)
- Sequential numbering of proposal IDs is possible

(4) Addressing incidents

Table 2-2-4-4 Uniswap: Response to Incident

Item	Summary	Supplementary information
Emergency Measures to incidents	- Core contract cannot be modified and cannot be suspended. - External contracts, interfaces, parameters, etc., other than the	- Core contract vulnerabilities, even if discovered, cannot be fixed - If the attack cannot be stopped from the outside, it cannot be defended against and can be fatal.

	core can be urgently modified by the development company	
Persons authorized to initiate emergency response	There are no specific rules, and there is no clear authority holder. - It is assumed that emergency measures will be implemented at the developer's own discretion	- In the event of an emergency, it is assumed that the developer will take action at its discretion, and the UNI holder's involvement will be limited.
Compensation for damages caused by incidents	Damage due to incidents, etc., is the responsibility of the user and no compensation will be provided (as specified in Terms of Service[55]).	- In the event of a major loss to a user, compensation from community funds may be proposed in a governance vote, etc., but may not be appropriately determined depending on the circumstances of the loss to the large UNI holder.

(5) Other

Table 2-2-4-5 Uniswap: Other Matters

Item	Summary	Supplementary information
Matters that can be implemented by the developer	Deployment of new version of smart contracts - Core contract upgrades are initiated by the development company	- The developer decides what new features to include in new versions, so there is a concern that the community's opinions will not be reflected.
	Modification of external contracts, interfaces, and parameters outside of the core - Some actions on matters passed by governance vote and some at the discretion of the developer (minor modifications, such as gas fee reductions).	- The code can be modified without going through the community at the discretion of the development company.
Anonymity of UNI holders	- UNI holders are, in principle, anonymous, making it difficult to identify the actual entity. - UNI holding addresses can be identified, but in many cases cannot be linked to real names because KYC is not performed	- Possibility that if a problem is discovered with a voting decision, the UNI holders involved in the decision making cannot be identified and the decision cannot be reversed or the decision makers cannot be held accountable.

2-2-5 Incident cases[56]

The following is an overview of the April 2020 incident case of the reentrancy vulnerability[57] , the reasons for its occurrence, and the issues involved.

(1) Date of Occurrence: April 18, 2020

(2) Damages: Approximately $300,000

[55] Uniswap Labs Terms of Service https://uniswap.org/terms-of-service

[56] https://peckshield.medium.com/uniswap-lendf-me-hacks-root-cause-and-loss-analysis-50f3263dcc09

[57] Reentrancy vulnerabilities are vulnerabilities that cause unauthorized execution of recursive processes (i.e., calling the same process again before the smart contract process is finished, causing the transfer to be executed multiple times before the balance is drawn, for example)

(3) Summary of Incident

- On April 18, Uniswap was subjected to a reentrancy attack by an attacker who stole approximately $300,000.
- On April 19, another DeFi protocol, Lendf.Me, was attacked using the same technique, and approximately $25 million was stolen.
- 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.

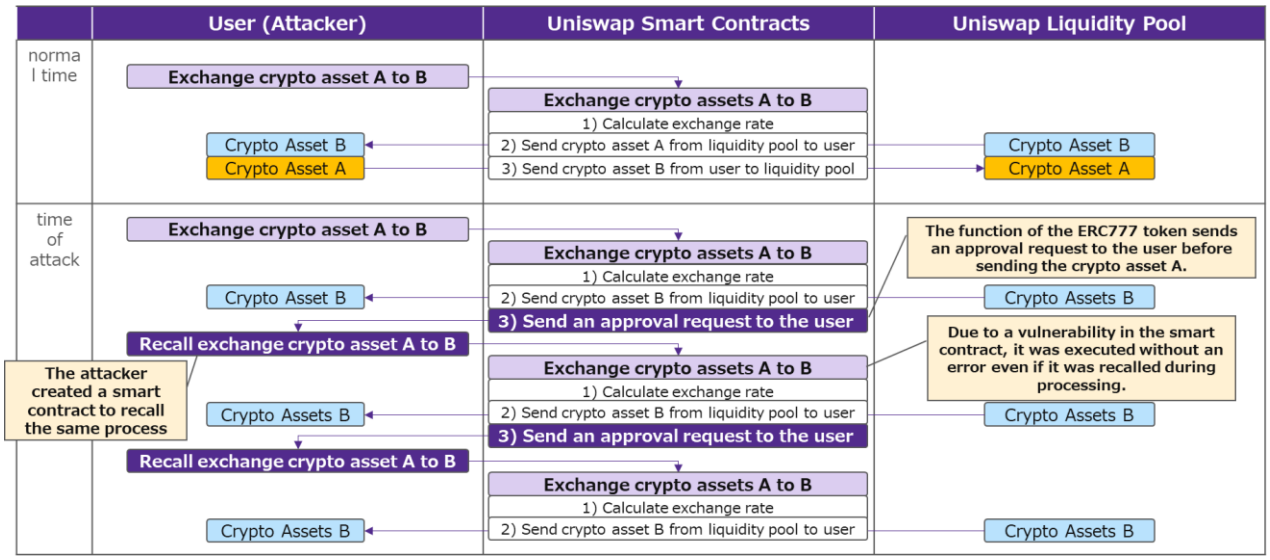


Figure 2-2-5-1 How the Uniswap Reentrancy Vulnerability Works

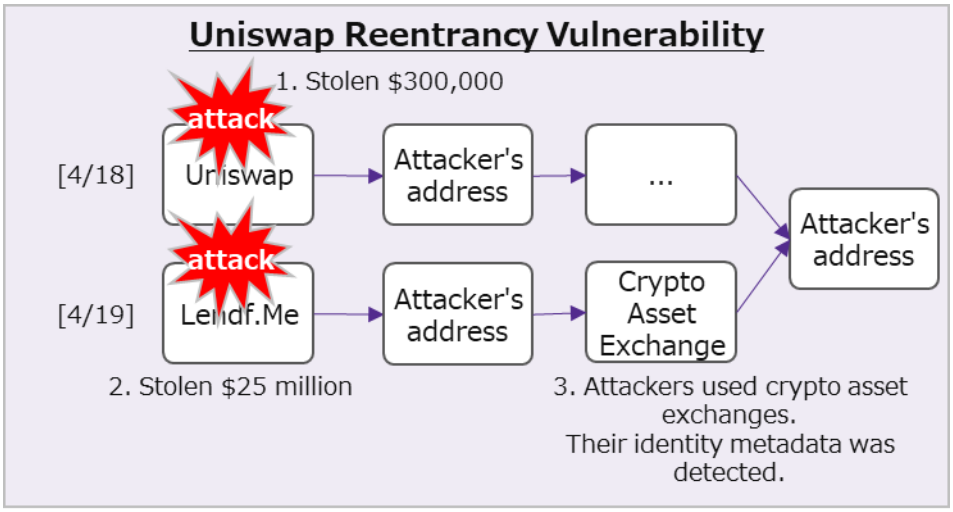


Figure 2-2-5-2 Outline of the attack

1. 4/18 Uniswap suffered a reentrancy attack and approximately $300,000 was stolen.
2. 4/19 Lendf.Me was attacked with the same technique and approximately $25 million was stolen.
3. 4/19 Attacker directly used the services of a crypto-asset exchange during a fund transfer and metadata of the attacker's identity was detected
4. 4/21 Identity of attacker revealed, Lendf.Me negotiated, 99% of funds returned

(5) Stolen funds and crypto-assets

Uniswap about $300,000 imBTC, ETH

Lendf.ME About $25 million WETH, USDT, HBTC, imBTC and 12 others in total

(6) Cause of Occurrence

Due to reentrancy vulnerabilities in Uniswap and Lendf.Me smart contracts

- There was a reentrancy vulnerability due to the lack of ERC-777 token support.
- 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.

(7) Incident Issues

Table 2-2-5 Uniswap Reentrancy Vulnerability Issues

Item	Sub-Item	Description of issues
Phenomenal Factor	Deployment	- There was a re-entrancy vulnerability in the ERC777 token. - Uniswap v1 was attacked by an attacker due to a reentrancy vulnerability caused by inadequate support for ERC-777 tokens.
Motivational Factors	Deployment	- Vulnerability in the source code was pointed out in the code audit, but it was decided to fix it in the next version and no immediate action was taken. - ConsenSys Code Audit Report in December 2018 (for immediate release)[58] , where this matter was noted. ➢ Severity: Major (the second most severe rank after Critical out of four.) ➢ There were a total of seven findings in the audit report, and this finding was the most significant. ➢ 3.1 Liquidity pool can be stolen in some tokens (e.g. ERC-777) - The vulnerability in this case had been pointed out to us before the incident occurred, but the plan was to address it in the next version of the software because then core contract can not be modified. ➢ Uniswap v1 core contract cannot be modified, so a change was made so that ERC777 tokens are no longer accepted. (Details unknown) ➢ The vulnerability has already been fixed in v2.
	Governance	- The vulnerability was pointed out in the code audit, but the code could not be modified due to the specifications of the core contract. - The results of the code audit were reported to Uniswap Labs (addressed to CEO Hayden Adams), and it is believed that the vulnerability was recognized by the development company management.

2-2-6 Uniswap Main Trust Points

(1) Uniswap Labs (Development Company)

- Based in NY, USA, the company is believed to develop and manage the Uniswap protocol and various tools, as well as operate user interfaces (websites, etc.).
- In light of the Company's plans to hire a community lead, it is assumed that the lead will have a certain degree of influence over the operation of the Uniswap community.
- Uniswap Labs approval would be required to implement the proposal as passed in the governance vote.

[58] ConsenSys Uniswap-audit-report-2018-12 https://github.com/ConsenSys/Uniswap-audit-report-2018-12#31-liquidity-pool-can-be-stolen-in-some-tokens-eg-erc-777-29

(2) Venture Capital

- Approximately 18% of UNI has been distributed to early investors, suggesting that some investors have a strong influence in governance voting.

(3) Code Auditing Company

- It is assumed that users trust the results of audits by code auditing companies and use the protocol.

(4) Wallet Provider

- Many users use a small number of non-custodial wallets such as Metamask (not only for Uniswap, but for DeFi in general), and the impact of a vulnerability in a wallet would be significant.

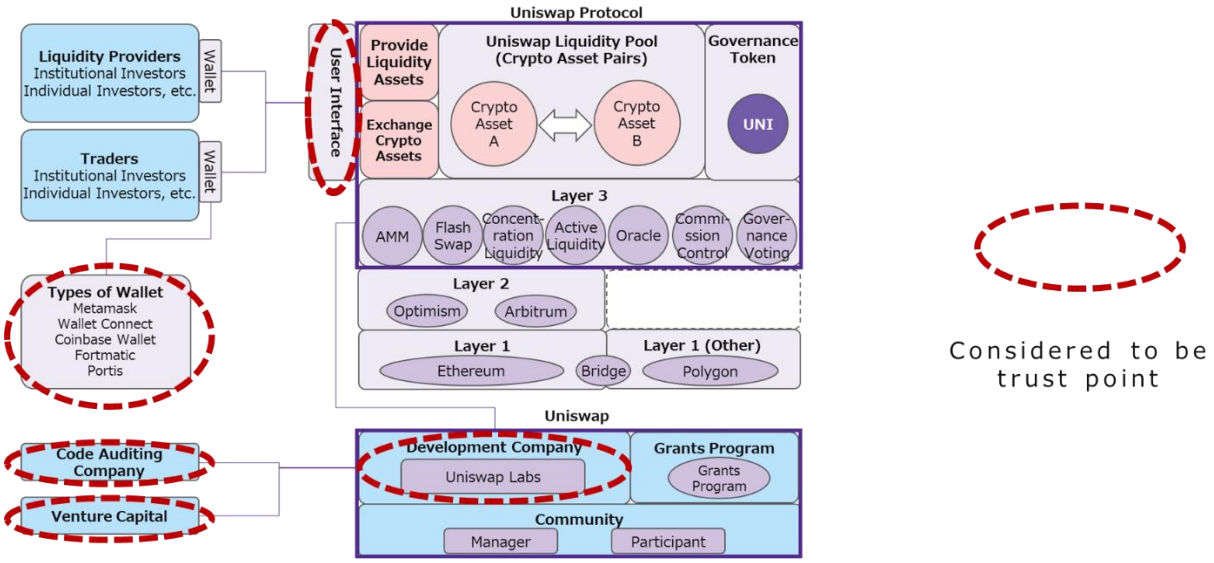


Figure 2-2-6-1 Main trust points (components) of Uniswap

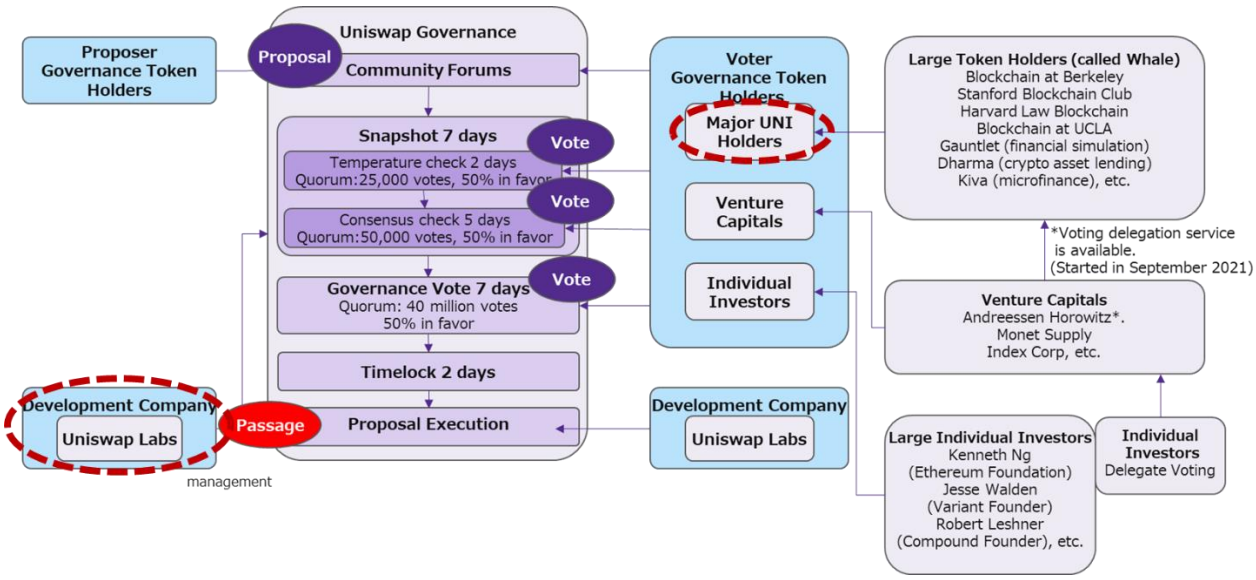


Figure 2-2-6-2 Uniswap Main Trust Points (Governance Voting)

2-3 Stablecoin Maker (DAI) Analysis

The survey research was conducted on the project overview, management organization, main technological characteristics, governance operations, and incident cases, with Maker as a studey target. Maker is characterized by the fact that the founding company, the Maker Foundation, was disssolved and transitioned to the MakerDAO, that it has established teams and rules for DAO operations by role, and that it is actively expanding into the real world in cooperation with financial institutions. The survey clarified the actual situation and analyze issues, problems, and risk matters in each of these areas.

2-3-1 Overall Project Overview

The main components of Maker, their mappings, and community overviews are shown in the chart and table below.

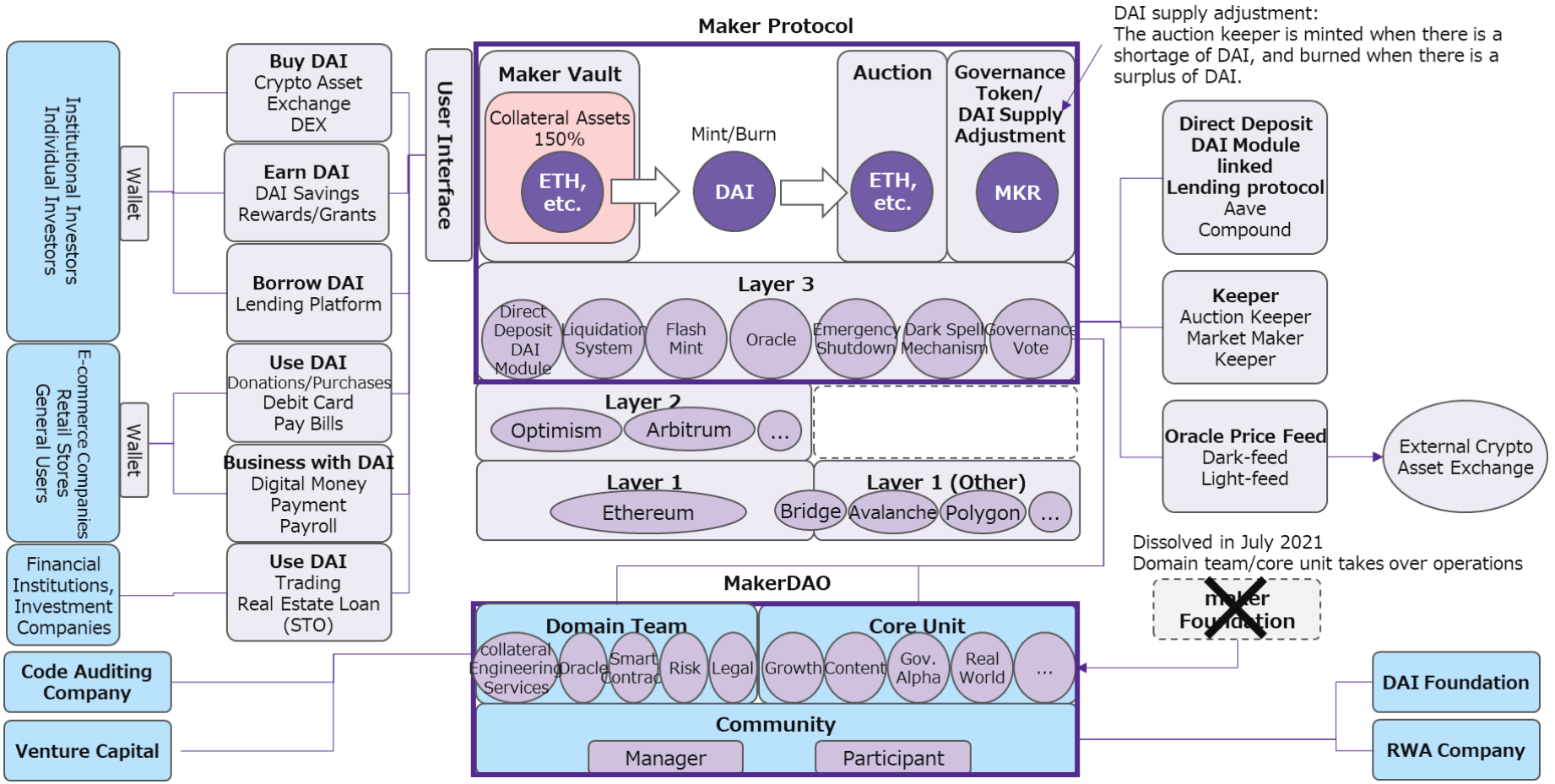


Figure 2-3-1-1 Main components of Maker

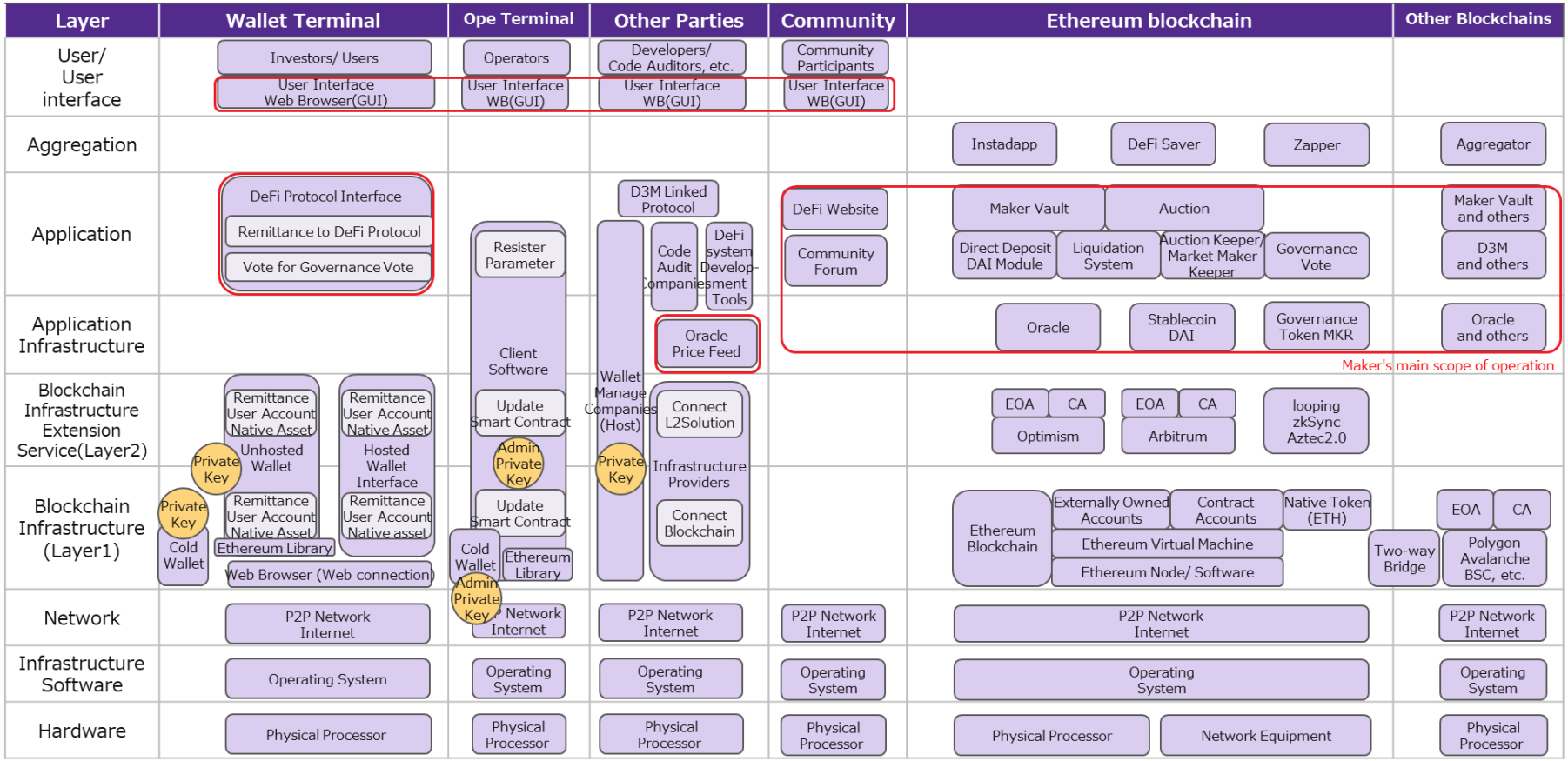


Figure 2-3-1-2 Mapping of Maker's main components

Table 2-3-1 Maker: Community and Related Corporations

Item	Summary	Supplementary information
Community (MakerDAO)	MakerDAO - On-chain voting by governance token MKR holders: 83,000 addresses - MakerDAO has two management teams as follows	- Founded in December 2014 - Based in: California, USA [59] - Founder: Rune Christensen - In July 2021, the Maker Foundation (Denmark) was dissolved and its assets was transferred to MakerDAO, a highly decentralized and autonomous organization.
	1) Domain Team (as of May 2022)[60] - Add collateral assets and design oracle mechanisms. i) Collateral Engineering Services Team Manage new collateral implementation and maintenance processes, including ii) Oracle Team Design of a new collateral type oracle feed mechanism, etc. iii) Smart Contract Team Adapter development and deployment of new collateral, etc. iv) Risk Team Risk analysis, etc., related to collateral types for which additional proposals have been made v) Legal Team Create collateral legitimate work product, etc. - Facilitators and contributors from each team leads the operation.	- Domain teams are comprised of independent individuals and others contracted by the MakerDAO. - On-chain voting approves domain team composition and personnel selection - The work of each team was inherited from the Maker Foundation. - Assume low quality risk at this time as many of the domain team will continue to be involved in code development and operations from the Maker Foundation.
	(2) Core units (as of May 2022)[61] 22 teams in total, with one facilitator from each team leading the operation - Real-World Finance - Risk - GovAlpha - Protocol Engineering - Growth - Sustainable Ecosystem Scaling - Oracles - Governance Communications - Dai Foundation - StarkNet Engineering - Collateral Engineering Services - Development and UX	- The Core Unit is comprised of independent individuals and others contracted by the MakerDAO. - On-chain voting approves the composition and selection of core unit members. - The work of each unit was inherited from the Maker Foundation. - Assumes low quality risk at this time as many of the core units are likely to continue to be involved in code development and operations from the Maker Foundation.

[59] https://www.crunchbase.com/organization/makerdao

[60] MIP7: Onboarding and Offboarding Domain Teams (Collateral Onboarding)
https://mips.makerdao.com/mips/details/MIP7#sentence-summary

[61] MIP38: DAO Primitives State https://mips.makerdao.com/mips/details/MIP38#makerdao-shop-mds-001-

	- Strategic Happiness - Data Insights - Deco Fixed-Rate - Immunefi Security - Sidestream Auction Services - Strategic Finance - TechOps - EVENTS - Content Production - MakerDAO Shop	
Affiliated Company	RWA Company LLC[62] - The goal is to connect the traditional credit market to MakerDAO to extend the collateral for generating DAI in the Maker protocol (Maker Vault) from crypto-assets to real assets. - Representing the Maker community and helping clients (loan originators, etc.) borrow capital (DAI) at a lower cost of capital through the Maker Vault - Conclusion of various contracts with clients on behalf of DAOs who have difficulty becoming a contracting entity, etc. - Ensure transparency by providing reports to MKR holders	- Founded in May 2021 - Location: Cayman Islands (under the Foundation Company Law of the Cayman Islands) - CEO: Gregory Di Prisco, former Maker Foundation Business Development Lead
	DAI Foundation[63] - A corporation to protect the Maker community's intellectual property (trademarks, domain names, software, SNS accounts, etc.) - In early 2020, the Maker Foundation transfers trademark rights of Maker and DAI to DAI Foundation.	- Founded in January 2020 - Location: Denmark[64] - Chairman: Solen PeterNielsen, former Head of Product at Maker foundation - The Board of Directors consists of six members.

2-3-2 Main Technological Characteristics

(1) Maker Vault [65]

- 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[66] and the community (Instadapp, Zerion, MyEtherWallet, etc.) makes it easy to access to the Maker Vault.

[62] RWA Company https://www.rwa.company/

[63] The DAI Foundation https://daifoundation.org/

[64] Announcing the Dai Foundation https://forum.makerdao.com/t/announcing-the-dai-foundation/1046

[65] Makerdao Whitepaper Maker Vaults https://makerdao.com/en/whitepaper/#maker-vaults

[66] https://oasis.app/

- 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.
- The liquidation ratio is selected by on-chain voting for each collateral asset: around 150% for ETH, 101% for USDC, etc.[67] .

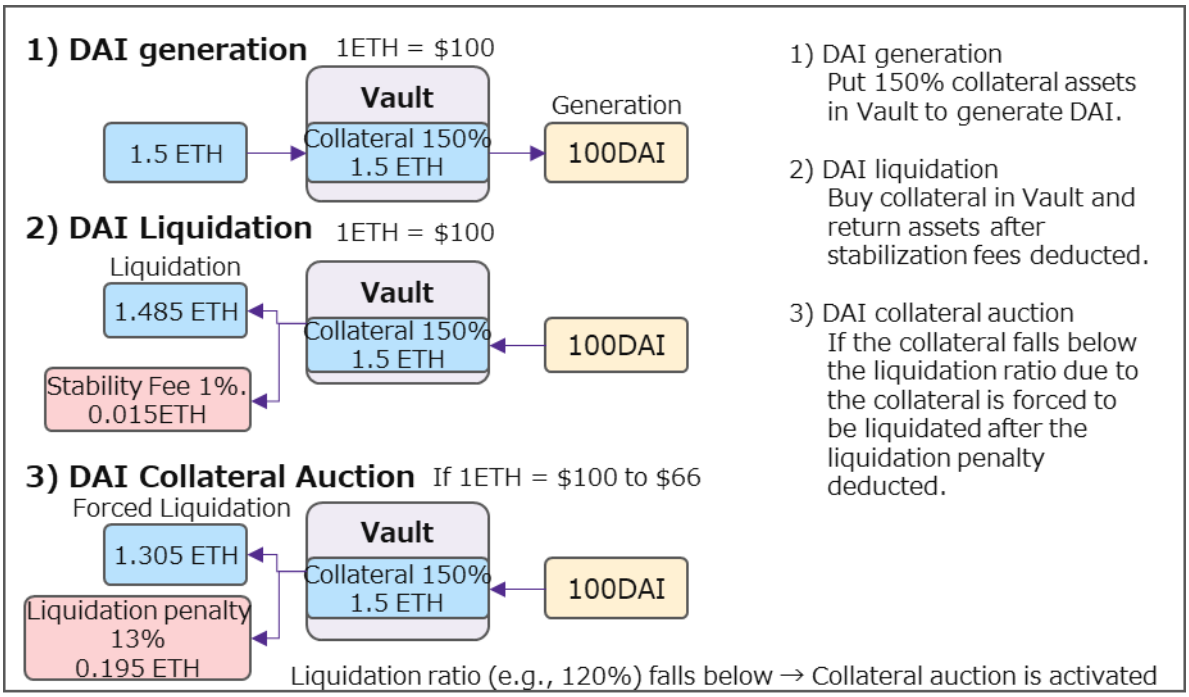


Figure 2-3-2-1 Maker Vault Overview

(2) Stablecoin DAI[68]

- Convert ETH to stablecoin DAI or DAI to ETH.
- ETH is not an ERC20 token, so it is converted to an ERC20 internal token within the Maker protocol before trading with others.
- For depositing funds into the Vault collateral rules and clearing funds through Auction, Maker prortocol internal tokenare used to exchange to avoid influence of external market prices.

Table 2-3-2 Maker: Summary of Stablecoin DAI

Item	Summary	Supplementary information
Generate DAI	- Generate DAI (crypto-asset-backed stablecoin) issued by locking excess collateral into the Maker Vault ➢ MCD: Multi Collateral DAI Support multiple collateral assets - Soft-pegged to USD. 1DAI = 1USD - DAI savings rate (DSR) is determined by on-chain voting	- The collateral to be deposited with Vault depends on the collateral assets. If the collateral ratio (liquidation ratio) is 150%, collateral equivalent to at least 150 USD is required to generate 100 DAI - The main collateral assets supported and the share of each asset in the total amount of collateral layers.[69] ➢ USDC (51.5%)

[67] https://daistats.com/#/collateral

[68] https://makerdao.world/en/learn/Dai

[69] https://daistats.com/#/overview

		➢ ETH (22.3%) ➢ WBTC (6.6%) ➢ USDP (5.3%), (as of April 2022)
Buy DAI	- Exchange for fiat currency at crypto-asset exchanges - Exchange for cryptocurrency on a crypto-asset exchange - Exchange at DEX ➢ Uniswap, 1inch Exchange, etc. - Exchange in the P2P marketplace ➢ Local Cryptos, Local Bitcoins, Bisq, etc.	-
Earn DAI	- Interest income ➢ Earn interest by locking your DAI holdings into a DSR (DAI Savings Rate) contract contract ➢ Access via various connection methods to the Oasis Portal or Maker protocol ➢ Parameters related to DAI savings rate determined by on-chain governance ➢ If DAI exceeds 1USD, MKR holders are incentivized to lower DSR to reduce demand, and if DAI is less than 1USD, MKR holders are incentivized to raise DAI to stimulate demand. - Rewards ➢ Bug bounties (rewarding those who find protocol bugs), etc. - Grants ➢ Maker's development grant programs (e.g., Gitcoin Grants) - Lending on lending platforms, etc. ➢ Lending DAI on platforms such as Compound, AAVE, dYdX, etc. - Hackathon ➢ MakerDAO Hackathon Initiative, etc. - Video Game Tournaments ➢ Axie Infinity (tournament reward)	-
Borrow DAI	- Borrowing through Maker or third-party lending platforms, etc. ➢ Borrow DAI with required collateral on platforms such as Oasis Borrow, Compound, AAVE, and dYdX	-

Use DAI	- Donations to Charity ➢ UNICEF, NeedsList (disaster relief), PoolDai (charitable organization donation fund), etc. - Online purchase (e-commerce) ➢ OpenSea (NFT), Decentraland (land on virtual space), Gods Unchained (digital goods), etc. - DAI Debit Card ➢ Crypto.com, Fold App (buy bitcoin), Monolith (connect Visa debit card to non-custodial wallet), Wirex, etc. - Gaming and Gambling ➢ CelerX (eSports), Pool Together (lottery) - Purchase Gift Cards ➢ Bidalli - Bill Payment ➢ Gold Plus Energy (U.S.-Texas, electricity payment), living Room of Satoshi (Australia)	- Possibility of gradual increase in use in the real world as well as in the crypto-asset market
Receive DAI	- Coinbase Commerce (digital money payment) - Ching-Store (mobile store) - Request Network (Billing Process) - GILDED (on-chain accounting services)	-
Payroll by DAI	- Whisp Money (payroll solution without KYC) - Sablier	- Some communities (Concource Open Community) use DAI to pay outside employees whose identities are difficult to guarantee, such as those working remotely from outside the country.

[Reference: Conversion of stablecoin DAI[70]]

ⅰ) ETH to WETH
ETH is not an ERC20 token, so it is converted to WETH (Wrapped ETH), an ERC20 token, so it can be traded with others. 1ETH = 1WETH

ⅱ) WETH to PETH
WETH is converted to PETH (Pooled ETH) and pooled as collateral in the Vault.
PETH is a crypto-asset dedicated to MakerDAO Converted by Maker's internal rate (1 WETH = 1.04 PETH, etc.).

ⅲ) PETH to DAI
Generate DAI based on PETH. Converted by rate (from DAI/ETH market price).

ⅳ) DAI to SIN
When liquidating DAI, it is converted to SIN before liquidation. 1DAI = 1SIN

[70] MakerDAO Tokens Explained: DAI, WETH, PETH, SIN, MKR. Part 1 https://medium.com/coinmonks/makerdao-tokens-explained-dai-weth-peth-sin-mkr-part-1-a46a0f687d5e

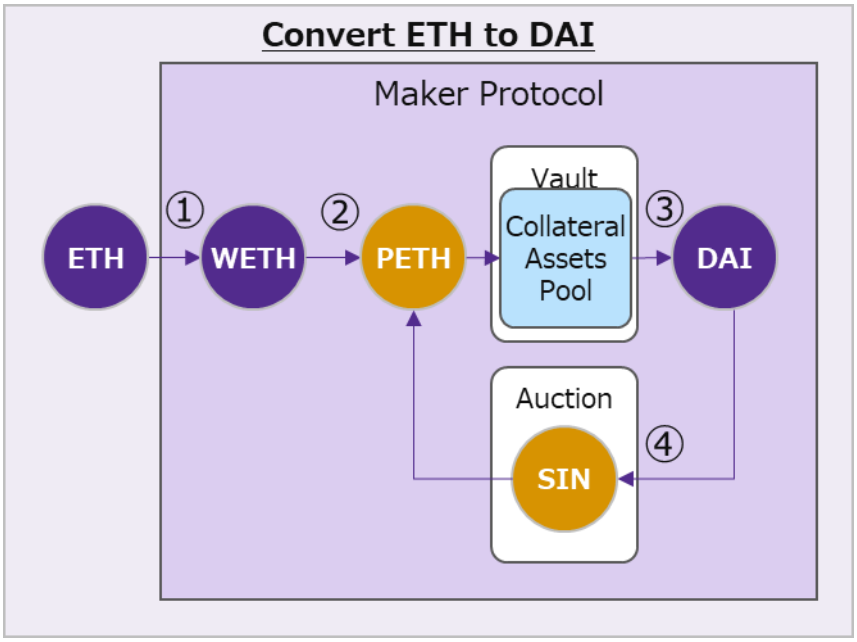


Figure 2-3-2 Maker Stablecoin DAI Conversion

(3) Direct Deposit DAI Module (D3M)[71]

- 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).

[71] Maker Direct Deposit Dai Module (D3M) https://governance.aave.com/t/the-maker-direct-deposit-dai-module-d3m/3514

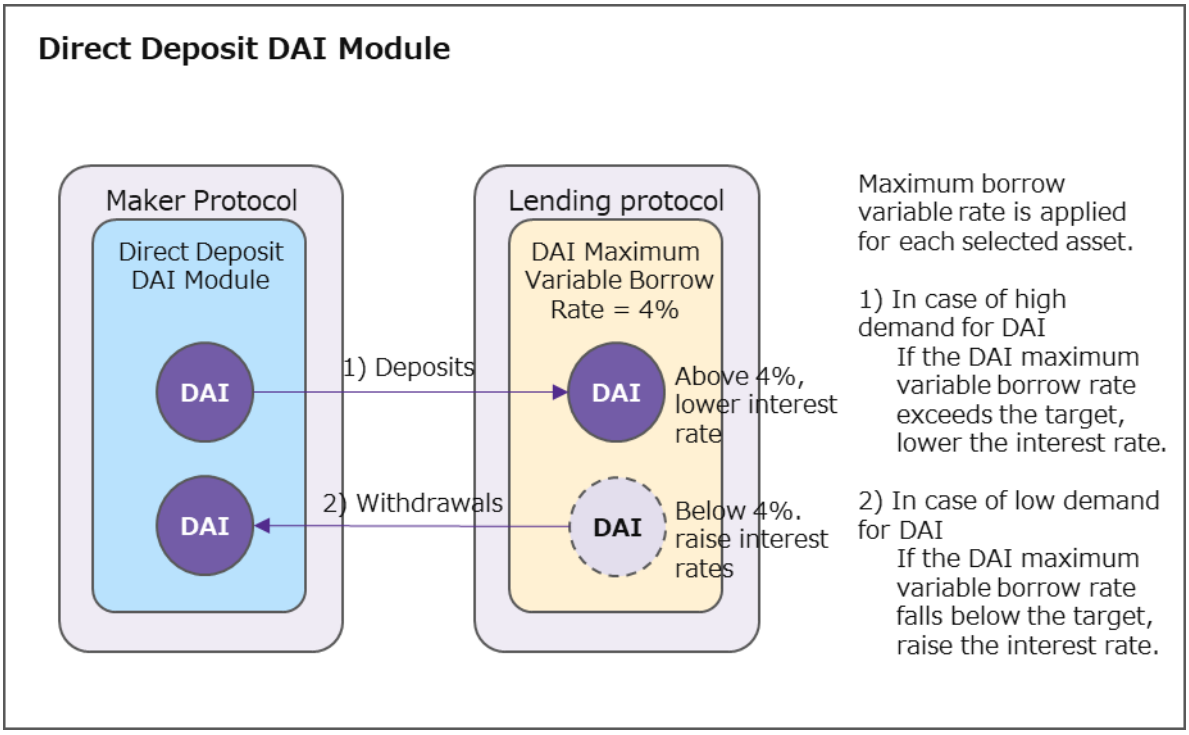


Figure 2-3-2-3 Maker D3M Overview

(4) Liquidation System 2.0[72]

- 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 clearing mechanism for Dutch auction method launched in April 2021.
  Auction bids are reduced until collateral is purchased
- 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.
- Auction bidding times and bid reduction rates are selected by on-chain voting.

[72] Maker Protocol Technical Docs Liquidation 2.0 Module https://docs.makerdao.com/smart-contract-modules/dog-and-clipper-detailed-documentation

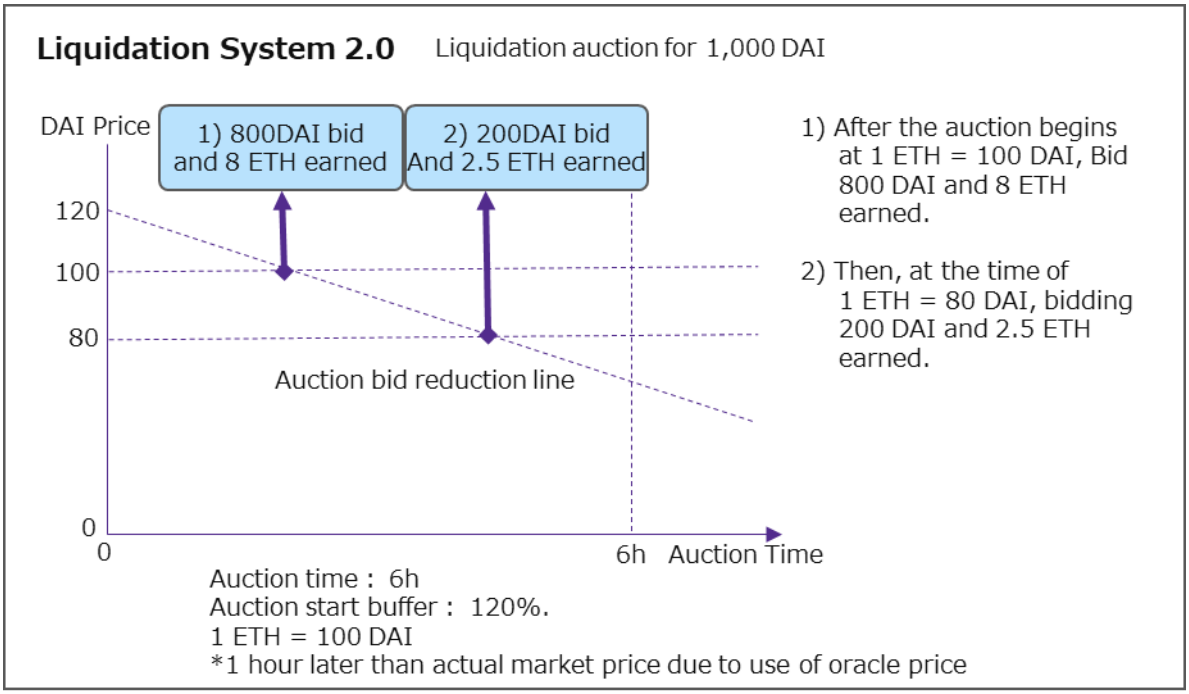


Figure 2-3-2-4 Overview of Maker Liquidation System 2.0

(5) Oracle management[73]

- 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 feed (refer to 24 external market prices such as Aave, Compound, Uniswap, etc. at[74] (as of April 2022)) 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 attacks (e.g., when collateral asset prices drop significantly, it is possible to take measures such as pledging additional collateral to avoid liquidation).
- The referenced price feed destinations, etc. are selected by on-chain voting.

[73] Makerdao Community oracle https://github.com/makerdao/community/blob/master/faqs/oracles.md

[74] MIP10c17: Subproposal for List of Feeds https://github.com/makerdao/mips/blob/master/MIP10/MIP10c17-List-of-Feeds.md

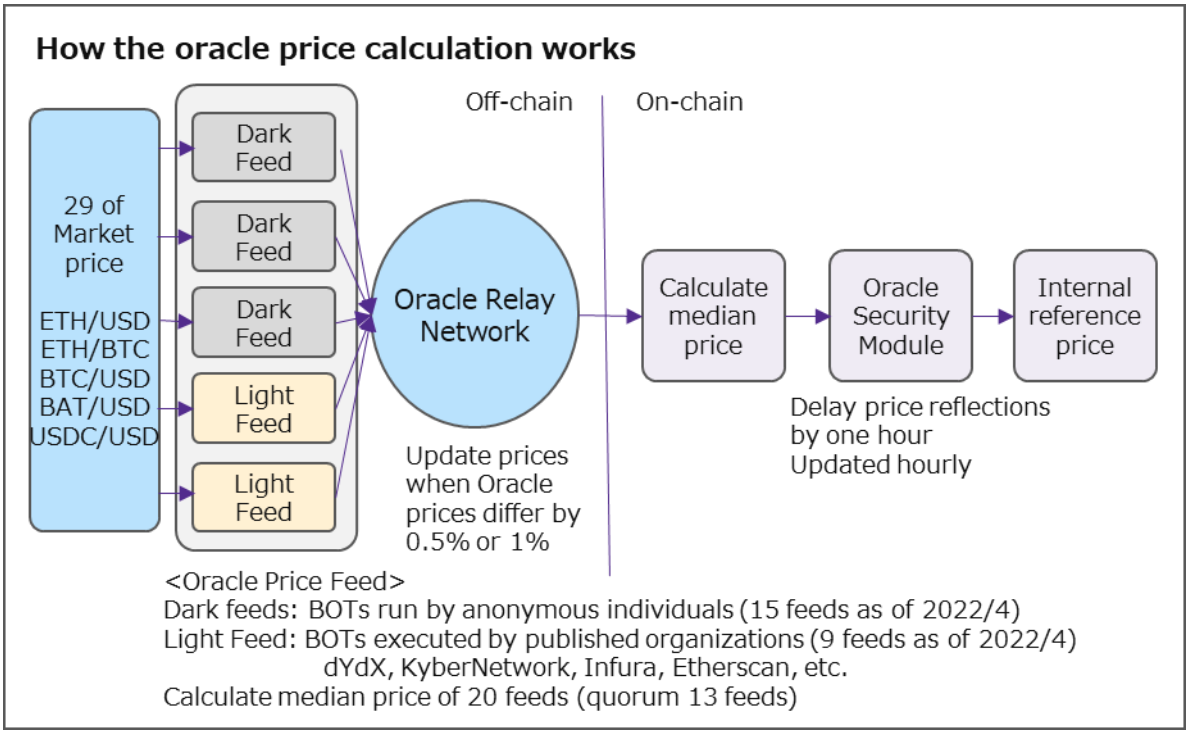


Figure 2-3-2-5 Maker Oracle Management Overview

(6) Maker Protocol Auction

- Upon forced liquidation, the Maker Protocol acquires the liquidated vault collateral and sells it using an auction mechanism.

Table 2-3-2-6 Maker: Protocol Auction Summary

Item	Summary	Supplementary information
Maker Protocol Auctions[75]	1) Surplus Auction 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 2) Debt auctions When DAI is insufficient for outstanding obligations, MKR tokens are issued and sold to bidders to secure DAI 3) Collateral auction Forced liquidation of collateral by charging a liquidation penalty in the event of collateral shortages due to falling token prices, etc.	-

(7) Keeper

Table 2-3-2-7 Maker: Keeper Summary

[75] Maker Protocol Technical Docs The Auctions of the Maker Protocol Auctions https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol

Item	Summary	Supplementary information
Keeper[76]	- Keepers are external agents (mainly BOTs) that run automatically for arbitrage according to an algorithm - Market Maker Keeper ➢ 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[77] - Auction Keeper ➢ Participate and bid in surplus, debt, and collateral auctions	- Market Maker Keeper automatically executes trades by referencing the market price on the designated exchange.

(8) Flashmint

Table 2-3-2-8 Maker: Flashmint Overview

Item	Summary	Supplementary information
Flashmint[78]	- DAI can be created under the condition of borrowing and returning (including fees) in one transaction. - Arbitrage opportunities available with no collateral required	- There is a debt limit (DAI/ETH: 15 billion ETH, etc.)

(9) DAI Savings Rate (DSR)

Table 2-3-2-9 Maker: Summary of DAI Savings Rates

Item	Summary	Supplementary information
DAI Savings Rate (DSR)[79]	- Any DAI holder can earn interest on their savings. - Access via Oasis Save Portal or Maker Protocol Gateways - The parameters that determine the amount of money a DAI holder gets are determined by on-chain governance - If DAI exceeds 1 USD, MKR holders lower their DSR; if DAI is less than 1 USD, MKR holders raise their DAI.	-

[76] Maker Protocol Technical Docs The Auctions of the Maker Protocol Keepers https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol

[77] MakerDAO market-maker-keeper https://github.com/makerdao/market-maker-keeper

[78] Maker Protocol Technical Docs Flash Mint Module https://docs.makerdao.com/smart-contract-modules/flash-mint-module

[79] Makerdao whitepaper The DAI Saving rate https://makerdao.com/en/whitepaper/#the-dai-savings-rate

(10) GSM (Governance Security Module)

Table 2-3-2-9 Maker: Overview of GSM

Item	Summary	Supplementary information
GSM[80]	- 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. - 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)

(11) Dark Spell Mechanism

Table 2-3-2-10 Maker: Overview of Dark Spell Mechanism

Item	Summary	Supplementary information
Dark Spell Mechanism[81]	- Mechanisms for modifying smart contracts to fix critical vulnerabilities - Apply protocol fixes without downtime - Work Process 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.) 2) Communicate dark spells to certain members in the community and trusted third parties. 3) Trusted third party quickly coordinates discussions and recognizes votes. 4) Trusted third party directs the governance facilitator to schedule a voting. 5) Wait for GSM delay period after voting is scheduled and passed.	- Interested parties ➢ Smart Contract Domain Team ➢ Governance Facilitator ➢ Trusted Third Party (selected by on-chain voting. Currently not registered) ➢ Certain members of the Maker community (not to be disclosed) - A different process than regular governance and executive voting ➢ Voting time is set to 24 hours (fixed) ➢ No quorum or threshold for passage of the vote is defined.

[80] Makerdao whitepaper Governance of the Maker Protocol https://makerdao.com/en/whitepaper/#use-of-the-mkr-token-in-maker-governance

[81] Makerdao MIP15: Dark Spell Mechanism https://mips.makerdao.com/mips/details/MIP15#sentence-summary

	6) Apply the code modification after the GSM delay period has elapsed. 7) Trusted third party and smart contract domain team to create a darkspell post-mortem analysis and publish it to the entire community.	

(12) Emergency shutdown

Table 2-3-2-12 Maker: Summary of Emergency Shutdown

Item	Summary	Supplementary information
Emergency Shutdown[82]	- Ability to shut down the Maker protocol to protect it from malicious attacks or to facilitate Maker protocol upgrades. - MKR holder deposits MKR in the Emergency Shutdown Module (ESM), which is immediately executed when the threshold is exceeded. - Execution is done in 3 phases, followed by redeployment depending on the cause of the outbreak 1) Maker protocol shutdown Oracle Price Feed Frozen, Vault Owners Withdraw Assets 2) Auction processing after emergency stop After the shutdown starts, forced clearing by collateral auction starts, and the protocol stops after all auctions are completed. 3) DAI holder claims the remaining collateral DAI holders claim collateral directly at a fixed rate Vault holders have priority over DAI holders 4) Redeploy protocols according to the nature of the attack ➢ Governance Attacks Disable the attacker and redeploy with everything else intact ➢ Oracle Attack Fix the oracle module and redeploy with everything else intact ➢ Black Swan Event	- Threshold for initiating emergency shutdown is 75,000 MKR (as of January 2022) - Black Swan Event: A Major Surprise Attack - Difficult to countermeasure, such as oracle attacks and other highly coordinated external price manipulation, and there is no direct workaround

[82] Makerdao Whitepaper Emergency Shutdown https://makerdao.com/en/whitepaper/#emergency-shutdown

	Redeploy with new improvements ➢ Unreasonable emergency shutdown Disable the attacker and redeploy with everything else intact	

(13) Available platforms

Table 2-3-2-12 Maker: DAI Available Platforms

Item	Summary	Supplementary information
Layer 2 Solution	DAI is available in multiple Ethereum Layer 2 solutions - Optimism - Arbitrum - Loopring - zkSync - Aztec 2.0	-
Blockchain	DAI can be used on multiple blockchains (used by bridges)[83] - Ethereum - Avalanche - Polygon - Binance Smart Chain - Fantom - klaytn - xDAI - Harmony - Solana - Celo - Moonriver	-

2-3-3 Cooperation with financial institutions

Table 2-3-3 Maker: Cooperation with Financial Institutions

Item	Summary	Supplementary information
Cooperation with Financial Institutions	Launched custody and trading services (June 2021) - Sygnum Bank AG (Swiss digital bank) ➢ Announced the launch of custody and trading services for Maker and several other crypto-asset tokens. ➢ Usd Coin (USDC) banking services already in place	Tradable Crypto-assets: - Aave (AAVE), Uniswap (UNI), Aragon (ANT), Curve (CRV), Maker (MKR), Synthetix (SNX), 1inch network (1INCH)

[83] Avalanche Token Dai Stablecoin https://snowtrace.io/token/0xd586E7F844cEa2F87f50152665BCbc2C279D8d70

	Entered into the real estate loan market (October 2021) - Forge (digital assets subsidiary of Société Générale) ➢ Partnership in real estate loans through STO (Security Token Offering). ➢ As a "Security Token Refinancing" loan, the company proposes to refinance with OFH Security Tokens (Housing Finance Bonds), which are backed by real estate loans. ➢ The tokens are made in accordance with French law and will serve as collateral for a $20 million loan to be taken out by DAI.	- This is the first example of a well-established bank working with a MakerDAO on bond collateral. - For the DAI issuance plan, Forge lists six entities 1) Société Générale 2) Forge 3) MakerDAO protocol 4) Legal representative of MakerDAO 5) Role of the DIIS Group (French Fixed Income Investors) Securities Agent 6) Exchanges - French related laws are seen as a measure to clear real world legal requirements, as they require securities agents to secure loan liquidation, etc.

2-3-4 Governance Operations

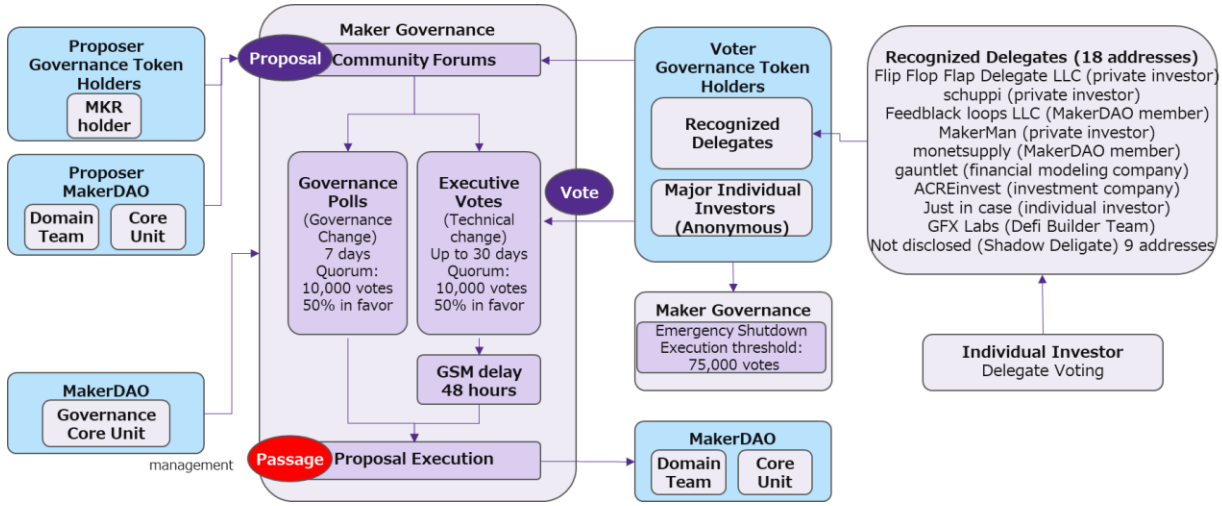


Figure 2-3-4 Governance Voting Process with MKR

(1) Community

Table 2-3-4-1 Maker: Community Basics

Item	Summary
Purpose of the community (summarized from official documentation)[84]	- MakerDAO is a decentralized governance community that enables the generation of DAI, the world's leading decentralized stablecoin. - The decentralized governance community of MakerDAO manages the generation of DAI through an embedded governance mechanism within the Maker Protocol. - MKR holders have the sole authority to enact changes to the system through voting.
Community	- Decentralized Autonomous Organization (MakerDAO) of Governance Token MKR Holders - The MakerDAO is managed by the Domain Team and Core Unit.

[84] MakerDAO https://makerdao.world/en/learn/MakerDAO

	- Domain team or core unit facilitator will lead the operation.

(2) Governance token (MKR)

Table 2-3-4-2 Maker Governance Tokens

Item	Summary	Supplementary information
Distribution of MKR[85]	MKR: 1 million tokens already distributed (as of January 2022) - Distribute a portion to early adopters - Sold a portion to VC (Andreessen Horowitz, Polychain Capital and others)	-
Number of addresses held by MKR[86] (as of Jan. 2022)	- Number of addresses held by MKR: 76,000 - Percentage of 1st place holdings: 17.39% - Percentage of top 10 addresses held 45.38%	- No undistributed portions locked to smart contracts, as is the case with UNI
MKR Features[87]	1) Voting rights in on-chain voting (governance tokens) 2) Resource for recapitalization - Additional supply of MKR when Maker Protocol becomes insolvent (upward price pressure on MKR) - Excess accumulation of DAI on the Maker Protocol balance sheet, exchanging DAI for MKR and burning MKR (upward price pressure on MKR)	- The function of 2) provides an incentive to maintain a healthy protocol for holders who expect the price of MKR to rise.

(3) Decision-making

Table 2-3-4-3 Maker: Decision-Making

Item	Summary	Supplementary information
Decision-Making Methods	- On-chain voting by MKR in two parts depending on the proposal 1) Governance Poll Decide on governance and DAO process other than technical changes to Maker protocol 2) Executive Vote Decide on technical changes to the Maker protocol. Make protocol changes such as DAI distribution according to the proposal and budget passed by voting 1). - Voting period:	- In the majority of voting 2), proposals of high importance involving protocol changes are being voted on in the governance voting decided in 1).

[85] Maker Profile https://messari.io/asset/maker/profile/launch-and-initial-token-distribution

[86] Etherscan Token Maker https://etherscan.io/token/0x9f8f72aa9304c8b593d555f12ef6589cc3a579a2

[87] MKR Token https://makerdao.world/en/faqs/mkr-token/

	➢ 1) 7 days, 2) up to 30 days ➢ 2) will be a continuous approval voting model, and if the number of votes for the latest successful proposal is exceeded, the proposal will be approved. If not, the proposal is rejected.	
Conditions for passage of governance vote (as of January 2022)	- Quorum 10,000 MKR (1% of total) - To pass: Majority of votes cast is in favor	-
Actual number of votes cast (2021)	1) 275 out of 307 approved (90% approval rate) 2) 47 out of 47 approved (100% approval rate)	-
Items that can be proposed in the Governance Vote	- MKR holders can participate in proposal and governance voting in forums such as ➢ Add new collateral asset types ➢ Change or add risk parameters ➢ DAI Savings Rate Changes ➢ Selecting Oracle Price Feeds ➢ Perform emergency shutdown ➢ Decided to upgrade system ➢ Payments for infrastructure and other services ➢ Voting can be outsourced to a published proxy	- Proposals will be discussed in the following 9 categories of forums 1) Update (notification of latest information) 2) Governance (General Governance) 3) Maker Protocol Improvement Proposals (MIP) (e.g., parameter changes) 4) Core Unit (various activities of the Core Unit) 5) Collateral on-boarding (addition of collateral assets) 6) Developers (tools and documentation) 7) Community Development 8) Employee Recruitment 9) Site feedback (Q&A on site use) - Proposals that have formed consensus opinion and received majority approval are sent for on-chain voting (decision made by Core Unit team)
Maker Vault risk parameters controlled by Maker Governance	- Examples of key risk parameters for Maker Vault 1) Debt limit Maximum amount of debt that can be created by a single collateral type 2) Stabilization fee Incurred at the time of DAI settlement (liquidation fee calculated from Vault's collateral assets and DAI generated) 3) Liquidation ratio The minimum required collateral ratio for a given collateral type. If the collateral ratio falls below the	-

	liquidation ratio, the liquidation process is initiated. 4) Liquidation penalty Additional fees collected at the time of liquidation 5) Maker Protocol Auction Duration Change the duration of debt and surplus auctions (maximum duration cannot be changed)	
Maker Governance Voters (as of January 2022)	- On-chain voting is done by voting proxies and individuals, but almost all voting is done by voting proxies. - Breakdown of voting proxies ➢ Total 18 addresses: 9 published, 9 not published (Shadow Delegate) ➢ Number of votes held: 98,500 (10.0% of total Jan. 2022) - The main published voting proxies are 1) Flip Flop Flap Delegate LLC (individual investor) 32,000 2) schuppi (individual investor) 20,000 3) Feedblack loops LLC 10,000 Tim Black, MakerDAO Community Contributor 4) MakerMan (private investor) 0.52 million 5) Monetsupply 0.5 million MakerDAO Risk Core Unit Core Contributor 6) gauntlet (financial modeling company) 3,000 7) ACREinvest (investment company) 1,000 8) Just in case (individual investor) 54 9) GFX Labs (DeFi Builder Team) 28 - In addition to the above, venture capitalists are also said to be involved. The following VCs were voting directly until 2019, but do not appear to be voting now[88] ➢ Andreessen Horowitz (California, USA) ➢ Field Technologies Inc. (Minnesota, U.S.A.)	- Two of the voting proxies are MakerDAO members, and together they hold 15,000 votes. These two members exceed the quorum (10,000 votes) for the proposal and are considered to have significant influence on the decision-making process through governance voting.

(4) Addressing incidents

Table 2-3-4-4 Response to Maker Incident

[88] Centralized Governance in Decentralized Finance (DeFi): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3971791

Item	Summary	Supplementary information
Emergency measures to incidents	- MKR holders deposit MKRs in the Emergency Shutdown Module (ESM), which immediately executes a shutdown when the threshold is exceeded. - Dark spell mechanism to fix critical vulnerabilities	- The emergency shutdown requires currently 75,000 MKR (being processed to raise it to 100,000), and voting proxies alone will not be able to reach 100,000 votes. The cooperation of many other MKR holders (individual voters) will be required. If the voting proxy is late or there are no other cooperating parties, it is assumed that it will be difficult to immediately defend against the attack - Dark spell mechanism takes a minimum of 3 days to fix the code, so there is concern that publicly known defects may not be addressed in time.
Persons authorized to initiate emergency response	- Emergency shutdown is triggered by MKR holder. - The Dark Spell Mechanism is activated by the Governance Facilitator.	- Dark Spell Mechanism has no publicly disclosed stakeholders, such as trusted third parties or community identifiers, and requires trust in authority figures
Compensation for damages caused by incidents	- Damage caused by incidents, etc. is the responsibility of the user and, in principle, no compensation will be provided (as specified in Terms of Use[89]). - Compensation for damages from the March 2020 incident was proposed for a governance vote, and the vote resulted in a decision not to compensate (since compensation would be made by printing more MKRs, which was opposed by major holders who were concerned about the price reduction of MKRs).	- The possibility that the status of the large MKR holders' damages will determine whether they support or oppose the governance proposal, and that equal judgment will not be exercised.

(5) Other

Table 2-3-4-5 Maker Governance Operations and Other Matters

Item	Summary	Supplementary information
Anonymity of MKR holders	- MKR holders are, in principle, anonymous, and it is difficult to identify the actual entity. - In many cases, MKR holding addresses can be identified but cannot be linked to real names because KYC is not performed - However, voting proxies can be identified as individuals or	- Possibility of not being able to identify the MKR holders involved in the decision-making process, making it difficult to revert the decision and hold the decision-maker accountable

[89] MakerDAO Terms of Use https://vote.makerdao.com/terms

	corporations because their attributes are made public.	

2-3-5 Incident Cases[90]

An overview of the March 2020 zero-bid attack incident case, the reasons for its occurrence, and the issues involved are presented as below.

(1) Date of Occurrence: March 12, 2020

(2) Damages: approximately $8.32 million

(3) Incident Summary

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.

(4) Case flow

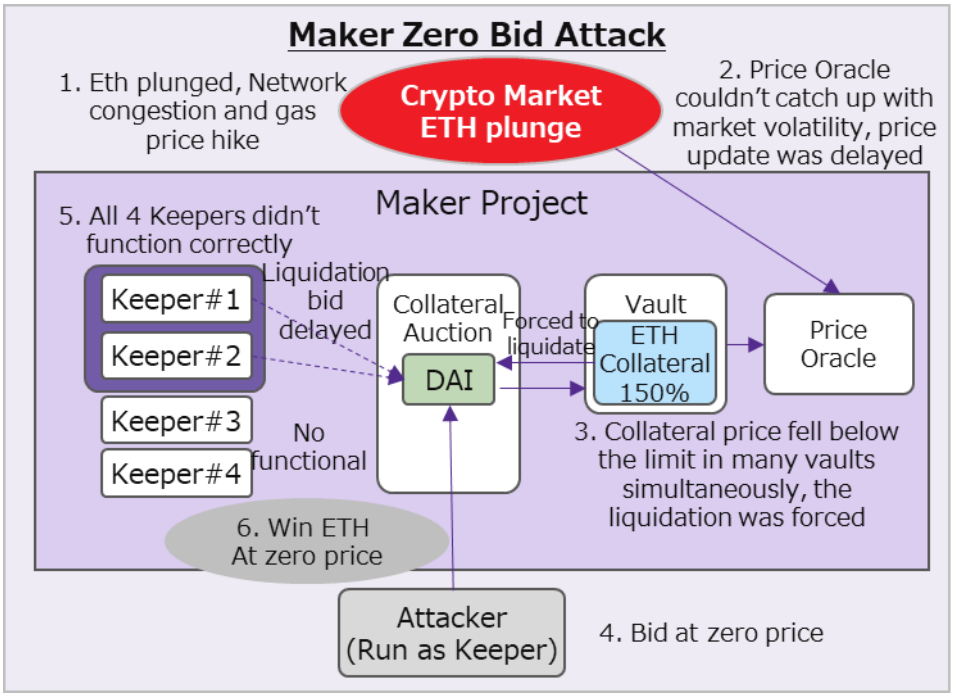


Figure 2-3-4-1 Maker Zero Bid Attack

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.
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.

[90] https://blog.makerdao.com/the-market-collapse-of-march-12-2020-how-it-impacted-makerdao/
https://insights.glassnode.com/what-really-happened-to-makerdao/
https://www.blocknative.com/blog/mempool-forensics
https://makerdao.com/en/whitepaper/
https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol#to-summarize-we-have-three-types-of-auctions
https://docs.makerdao.com/keepers/auction-keepers
https://www.coindesk.com/tech/2020/09/23/makerdao-users-hosed-by-march-flash-crash-wont-get-mkr-payouts-say-mkr-whales/

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.
4. In the collateral auction, the attacker set up a "zero bid" (exchanged DAI at zero value for ETH).
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.
    - Keeper#1, #2 Due to gas price spike, bid transaction was not processed within the time limit (10 minutes).
    - Keeper#3 Maker Foundation operated the system, but it did not work due to technical problems caused by network congestion.
    - Keeper#4 DAI to be cleared was exhausted and processing stopped for several hours.
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.)
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)

(5) Cause of Occurrence

- Gas price spike in Ethereum due to the ETH price collapse, which exploited the fact that Keeper was not working properly to set up a zero bid
- 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.[91]

(6) Incident Issues

Table 2-3-5 Problems with Maker Zero Bid Attacks

Item	Sub-Item	Description of issues	Existing Risks
Phenomenal Factors	Deployment	- Keeper auction bids could not be processed due to gas pricing issues - Keeper's gas prices are calculated based on average prices on Ethereum, but they could not keep up with the rapid increase in gas prices, and bid transactions were submitted at lower gas prices, which were not processed within the auction time limit.	- Legitimate auction bids are not passed while malicious bids are passed, resulting in zero bids and other attacks.
		- Oracle's price reflections delayed. - Network congestion and gas price spikes delayed the acquisition of market prices from multiple Oracle price feeds and delayed the internal reflection of ETH prices. - The Oracle price feed was operated by a BOT (dark feed) of several	- Oracle fails to reflect normal prices, resulting in a difference from the market price, which leads to an oracle attack

[91] Evidence of Mempool Manipulation on Black Thursday: Hammerbots, Mempool Compression, and Spontaneous Stuck Transactionshttps://www.blocknative.com/blog/mempool-forensics

		anonymous individuals, which caused delays in obtaining market prices due to the network being affected by congestion.	
	Platform	- High volume of transactions caused congestion in the Ethereum network and gas prices skyrocketed. - The increase in transactions due to the ETH price collapse and the large number of meaningless transactions (possibly intentional) caused network congestion, which led to the gas price spike.	- The increase in transactions causes processing delays and gas price spikes, which prevent normal transactions from going through and cause a variety of negative effects.
	Operation	- Attacker made zero bids during the processing of a collateral auction with forced liquidation of the Vault - The collateral auction was originally conducted by Keeper to buy DAI according to the internal market price, but the attacker's zero bid was accepted and passed the auction.	- Possible to accept zero bids depending on situations.
		- One of the Keepers was not functioning when the attack occurred. - Keeper#3 was operated by the Maker Foundation, but did not work due to technical problems caused by network congestion	- Auction bid processing capacity is reduced, resulting in processing delays and bidding failures.
		- When a large number of forced liquidations took place simultaneously, there were insufficient DAI assets to be used in the liquidation. - Keeper#4 was operating correctly, but did not function because a large number of forced liquidations were taking place at the same time, causing DAI to run out and bids could not be placed. At this point, ETH had collapsed and it was difficult to procure the DAI needed for liquidation.	- Depletion of collateral assets prevents mandatory liquidation and legitimate bidding.
Motivational Factors	Operation	- Failure to take precautions against attacks on collateral assets due to ETH price collapse, etc. - In this case, since ETH was the single collateral asset, the collapse of the ETH price caused DAI to be forced to liquidate, which had a significant impact. - The MakerDAO called the attack a "black swan event" (a serious surprise attack) and stated that there is no fail-safe solution to the attack, but a combination of proper governance and Maker protocols.	- Price manipulation of collateral assets causes massive forced liquidation and prevents legitimate bidding
		- There was no plan in place in case all Keepers were shut down.	- When Keeper is shut down, legitimate auction bids and arbitrage to

		- At the time of the attack, only four Keepers were in operation, and as a result, they were not all functional; the impact and measures if all Keeper systems were shut down was not considered in advance, causing the damage.	keep prices at 1USD are not performed. Abusive bidding and significant price fluctuations will occur.
	Governance	- On-chain voting was controlled by major MKR holders and losses were not compensated. - On-chain vote results in decision not to compensate investors for losses (Septenber 2020) - The vote was dominated by large MKR holders and was rejected by 9% of MKR holders (38 users). The compensation included printing more MKR tokens, and opposition to the additional issuance lowering the price outweighed the compensation proposal.	- On-chain voting may be controlled by large MKR holders and a few MKR holders may be harmed
		- Sued by investors who suffered losses in the case (April 2020). - 20 investors who lost their funds have filed a lawsuit against Maker's organization. Reason for the lawsuit alleged that the risk of losing all of their collateral due to Vault's forced liquidation was not explained to them. - Organizations subject to litigation, related parties ➢ Maker Foundation ➢ Maker Ecosystem Growth Foundation ➢ Dai Foundation ➢ Related parties including the Maker Foundation - Brought in the United States District Court for the Northern District of California by Plaintiff Peter Johnson, represented by Harris Berne Christensen LLP, Portland, Oregon. - September 25,2020 Defendant's (Maker) motion was granted and the case was stayed and assigned to the American Arbitration Association. Defendant's motion alleged that Plaintiff contracted to view the "DAI Terms of Use" upon signing up for the Maker platform.	- Even if the loss is caused by external factors of the market price collapse, it can be litigated if the loss is caused by reasons not attributable to the investor.
	Regulation	- The Ethereum network congestion was intentionally caused by an attacker, but there does not appear to be any criminal investigation, and the theft of $8.32 million has not been charged as a crime.	- Attacks against the DeFi project are less culpable and may increase crime

2-3-6 Maker's main trust points

(1) RWA Company, DAI Foundation (affiliated corporation)

The Maker Foundation was dissolved, but the RWA Company, which handles various contracts with clients, and the DAI Foundation, the management corporation for the intellectual property of the Maker community, continue to exist.

(2) Domain Team Core Unit (MakerDAO)

Domain teams and core units organized within the MakerDAO have taken over key operations of the Maker Foundation (code development, risk management, sales activities, etc.).

(3) Venture Capital/Voting Proxy

A portion of MKR has been sold to venture capitalists and other investors through an ICO, and it is likely that the initial investors have some influence on the governance vote.

Voting proxies at ・18 addresses have been delegated to vote by individual investors and have significant influence in governance voting. The holding entity for 9 addresses is not disclosed.

(4) Dark Spell Mechanism

A mechanism for domain teams to develop fix code and for certain persons in the community or trusted third parties to fix critical vulnerabilities under special authorization. Details of third parties, etc. are not disclosed.

(5) Keeper.

In order for mandatory liquidation to be properly handled in the event of a decline in collateral asset prices, it is a prerequisite that the keepers who bid on collateral auctions, etc., are functional, and if they are dysfunctional, it will cause the incidents described above.

(6) Code Auditing Company

It is assumed that users trust the results of audits by code auditing companies and use the protocol.

(7) Wallet Provider

Many users use a small number of non-custodial wallets such as Metamask (not just Maker, but DeFi in general), and the impact of a vulnerability in a wallet would be significant.

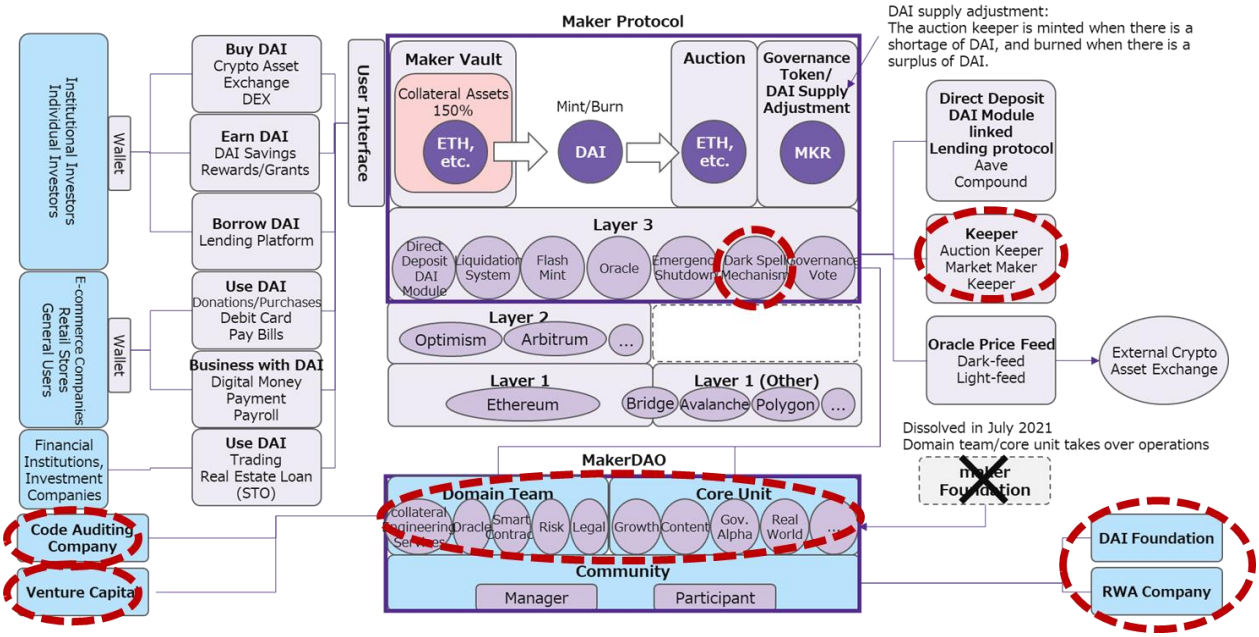


Figure 2-3-6-1 Maker's main trust points (components)

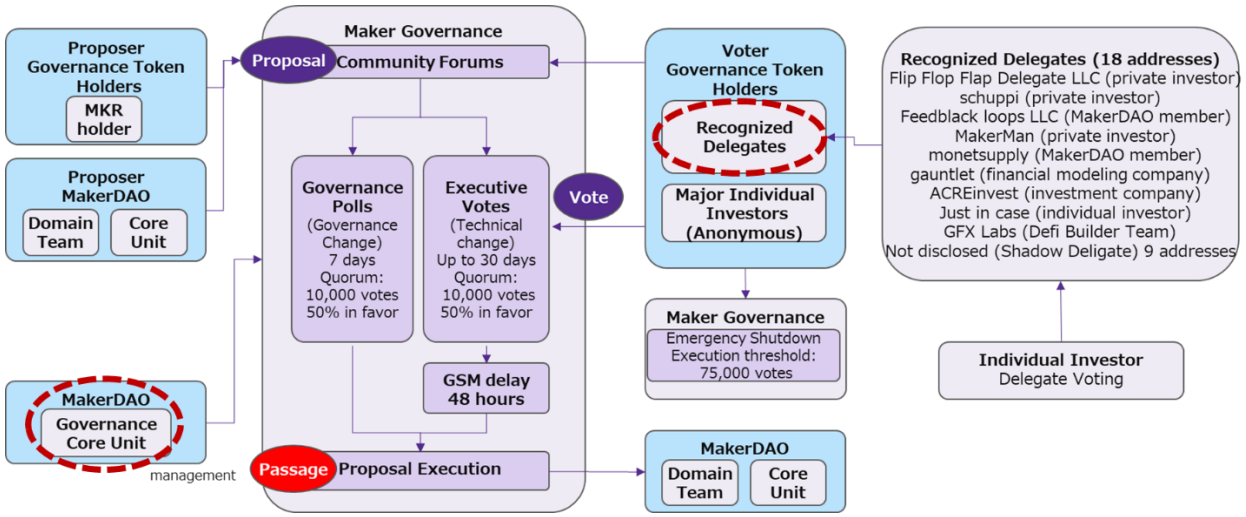


Figure 2-3-6-2 Maker's Main Trust Points (Governance Voting)

2-4 Lending Aave Analysis

Aave is a subject of a detailed research study, including a project overview, governing body, key technical characteristics, and governance operations. Aave, a lending protocol, offers advanced services such as DeFi services for institutional investors in cooperation with KYC providers and credit delegation, and is actively expanding into the financial market in cooperation with financial institutions. We clarified the actual situation through a study of each item and analyzed issues, problems, and risk matters.

2-4-1 Overall Project Overview

The main components of Aave, their mapping and community overview are shown in the figure and table below.

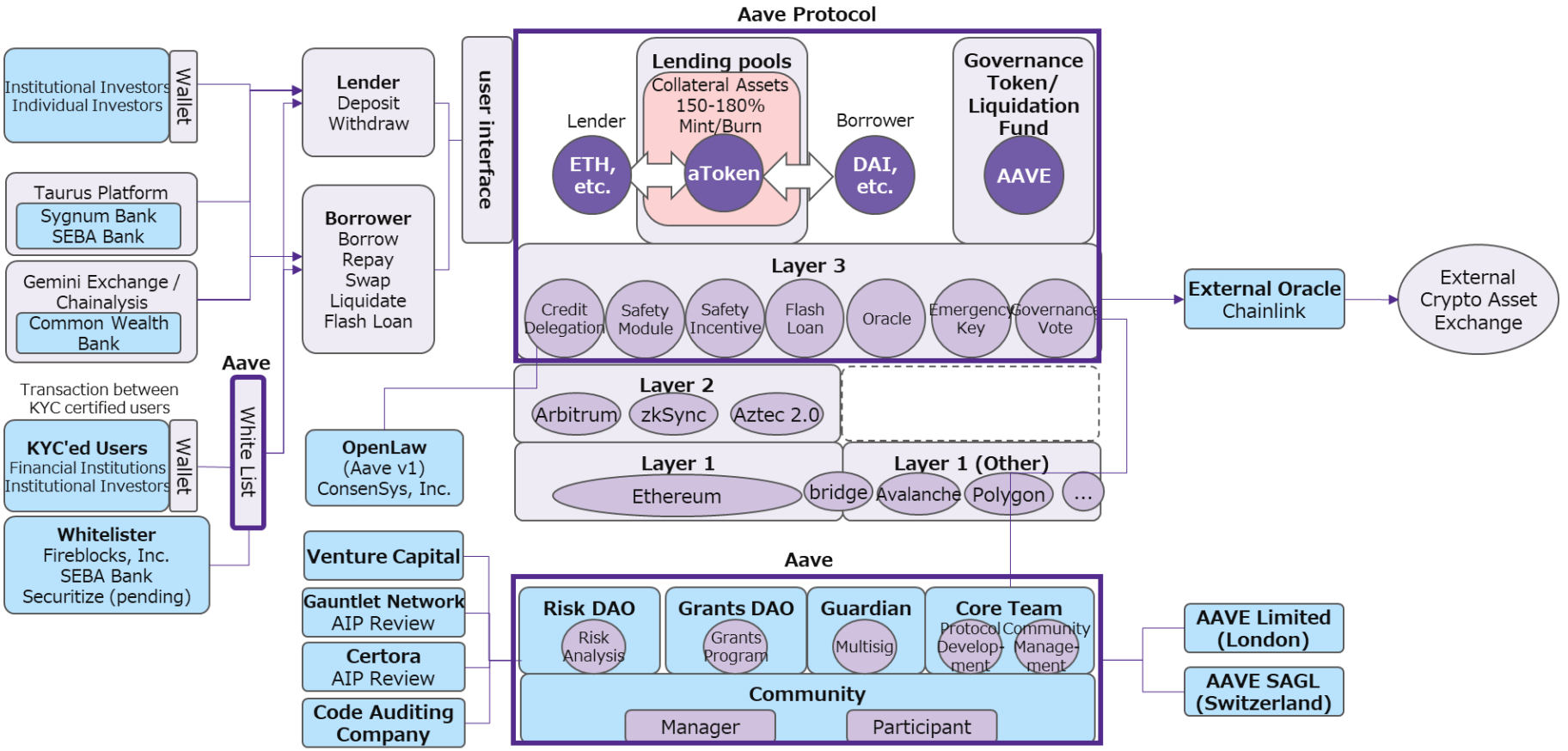


Figure 2-4-1-1 Main components of Aave

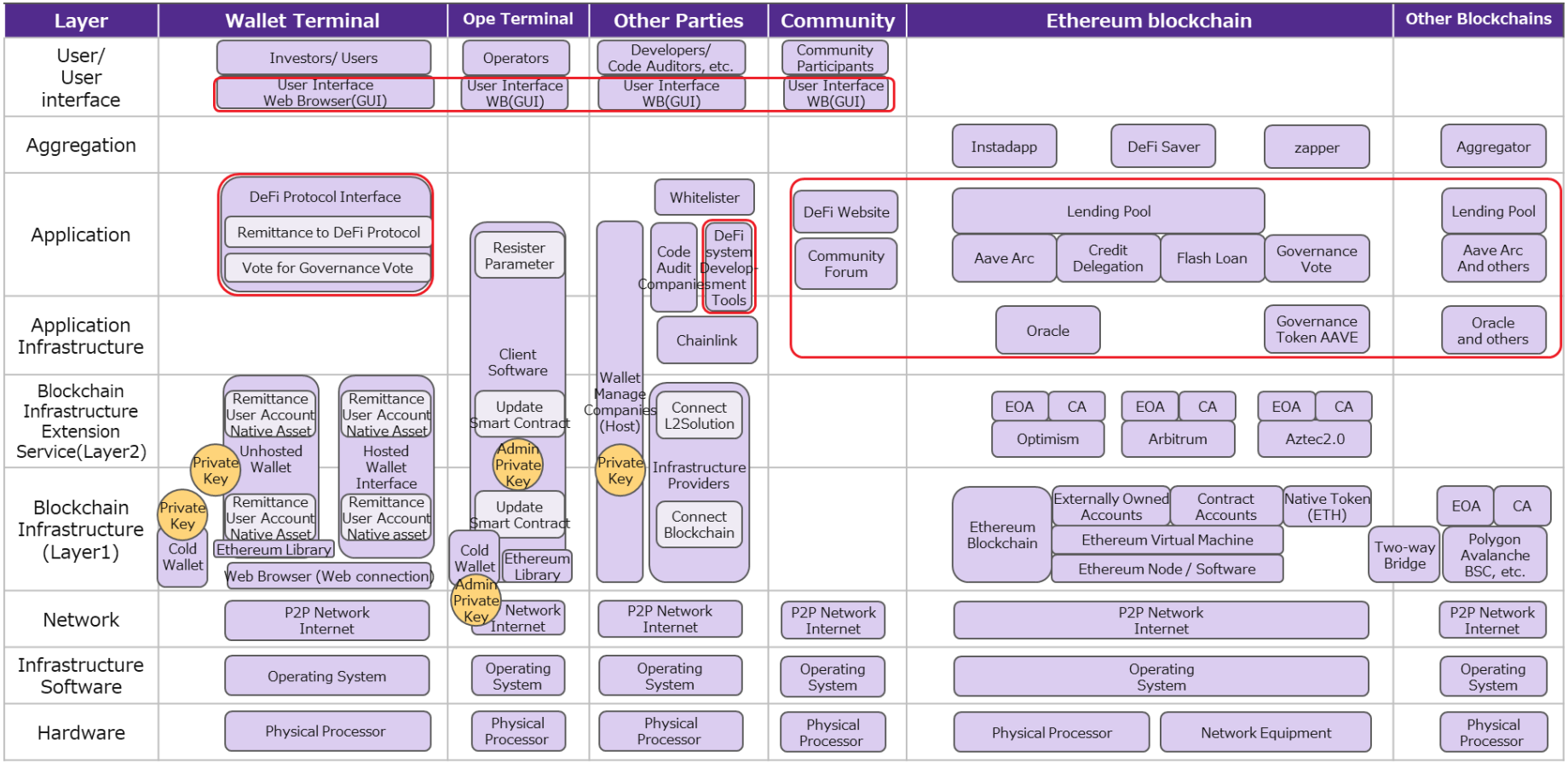


Figure 2-4-1-2 Mapping of Aave's main components

Table 2-4-1-3 Aave: Community, Developer, and Version Trends

Item	Summary	Supplementary information
Version and Main Functions	- 2017: Inauguration as ETHLend - 2018: Name changed to Aave. - 2020: v1 launch (ETHLend protocol no longer functional) - 2021: v2 launch - March 2022: v3 launch	-
Community	Aave Community (DAO) - Operated by governor token holders (number of addresses held: 100,000) - Further improve dispersion and independence in accordance with a policy called Aavenomics[92] - Aave Core Team manages the Aave community	-
affiliated company	<u>Aave Limited</u>[93] - Aave's U.K. subsidiary - Obtained approval from the Financial Conduct Authority (FCA) in the U.K. to operate as an "electronic money institution" (approved in July 2020). - Details of its activities as a legal entity are not known.	- Founded in May 2017 - Location: London - Founder: Stani Kulechov (Founder&CEO) - Operating members: 53 members located in the U.K., U.S.A., and other countries (Jan. 2022)[94] - At the time of the survey, there were no specific activities in the UK.[95]
	<u>Aave SAGL</u> - Switzerland - Details of activities are unknown.	- Founded in 2018 - Location: Switzerland (Chiasso) - Founder: Stani Kulechov (Founder&CEO)
Aave Core Team	- Develop and operate Aave protocols (code modification and related operations) and manage the community.	Lead: Stani Kulechov Aave management members share roles.
Aave Risk DAO (as of February 2022)	- Perform risk analysis and evaluation of Aave protocol and Safety module - Activities budget: $750,000 per year - Operating Fund Total of 6 multisig (4-of-6) to be determined - Nominated 3 RiskDAOs, 2 Gauntlet, and 1 Aave commmunity	- Managed by 7 members plus university students ➢ Project Management & Governance: monet-supply ➢ Market Risk Analysis: Thomas, Jack, Roberto, Jeremy ➢ Technical Risk: Mateusz ➢ Real World Asset Risk: Will ➢ Student Contributor: Blockchain at Berkeley
Aave Grants DAO	- A grant program that funds ideas submitted by the community, with a	Lead: - Shreyas Hariharan (Llama Founder, Uniswap grants)

[92] Decentralizing Aave https://docs.aave.com/aavenomics/

[93] Aave Limited https://aave.co.uk/

[94] RocketReach Aave Information https://rocketreach.co/aave-profile_b443387efa0db443

[95] The Financial Services Register https://register.fca.org.uk/s/firm?id=0010X00004U9vVAQAZ

(as of February 2022)	focus on empowering a broader network of community developers - Grant budget: $4 million per year - Operating budget: $500,000 per year - Committee: 8 members in total 1 lead, 7 reviewers	Reviewers: - Aleks Larsen, Blockchain Capital - Jose Maria Macedo, Delphi Digital - Imran Khan (DeFi Alliance) - Maggie Love (W3BCLOUD and SheFi) - Corbin Page (ConsenSys Codefi) - Nick Cannon (Gauntlet) - Calvin Chu (Independent)
Guardian (as of February 2022)	- Established as a community multisig to protect against potential governance hijacking by centralized actors. - Multisig runs 5-of-10 - Smart contract updates and emergency keys (protocol suspension) can be triggered. - It operates with 10 members, all of whom were elected in September 2021. - Proposed by Grants DAO lead (Shreyas Hariharan)	10 subjects - Arthur0x (DeFiance Capital) - Coderdan (Aavegotchi) - Gavi Galloway (Standard Crypto) - Isa Kivlighan (Aave community, previously head of marketing on the Aave Genesis team) - 0xMaki (Sushi) - Hilmar Maximilian Orth (Gelato) - Meltem Demirors (Coinshares) - Corbin Page (ConsenSys Codefi, Aave Grants DAO) - Imran Khan (DeFi Alliance, Aave Grants DAO) - Dennison Bertram (Tally)
Partner Company [96]	Gauntlet Network[97] - Provide a dashboard with recommended values for parameters that balance Aave's capital efficiency and risk - Participate as a risk contributor in the review of the Aave Improvement Proposal (AIP) for the Aave Governance Proposal	- Established in 2018 · Headquartered in New York, US - (32 employees as of Mar. 2022)
	Certora[98] - Perform a code audit of the Aave protocol. - Participate as a security contributor in the review of the Aave Improvement Proposal (AIP) for the Aave Governance Proposal	- Founded in 2019 Headquartered in Tel Aviv, Israel - 37 employees (as of Mar. 2022) - Aave Founder Stani Kulechov Joins Advisory Board

2-4-2 Main Technological Characteristics

(1) Overall view of the protocol[99]

- 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).

[96] Aave Developers Governance Guide https://docs.aave.com/developers/guides/governance-guide

[97] Gauntlet Networks, Inc. https://www.crunchbase.com/organization/gauntlet

[98] Certora Inc. https://www.crunchbase.com/organization/certora

[99] aave-v2-whitepaper https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf

- When crypto-assets are deposited into the Lending Pool, the pool receives aToken[100] (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)[101] .
- 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.

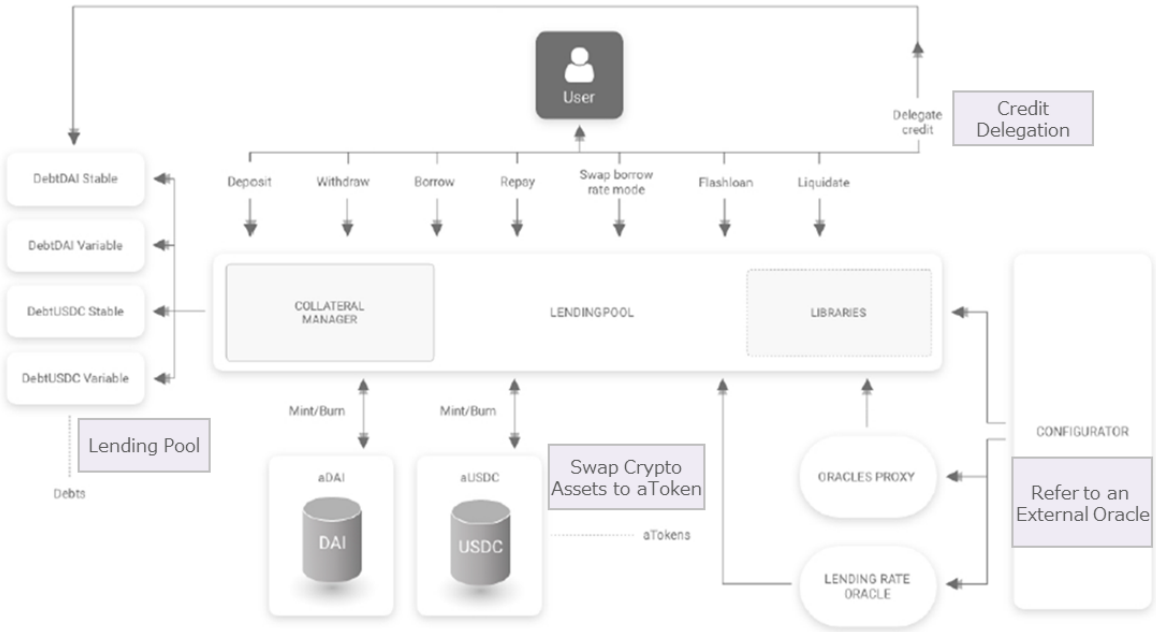


Figure 2-4-2-1 Aave: Overall view of the protocol

(2) Aave interest bearing tokens (aToken)[102]

- When a crypto-asset is deposited, a token with an a in the initial letter of the crypto-asset is generated at a 1:1 ratio and burned when the crypto-asset is withdrawn.
- For example, depositing 1 ETH generates 1aETH token, and burning 1aETH returns 1 ETH.
- aToken has the advantage of being able to grant interest directly in real time without gas fees within the Aave protocol.

(3) Liquidation[103]

- Liquidation occurs when the value of crypto-assets deposited in the lending pool by users falls below a predetermined collateral ratio due to a decline in the value of crypto-assets or an increase in the value of crypto-assets borrowed.

---

[100] Aave AToken https://docs.aave.com/developers/tokens/atoken

[101] Price Oracle https://docs.aave.com/developers/v/2.0/the-core-protocol/price-oracle

[102] Aave Developers aTokens https://docs.aave.com/developers/v/1.0/developing-on-aave/the-protocol/atokens#:~:text=The%20aTokens%20are%20interest%2Dbearing,safely%20stored%2C%20transferred%20or%20traded .

[103] Aave FAQ Liquidations https://docs.aave.com/faq/liquidations

- In liquidation, up to 50% of the collateral is refunded and a liquidation fee is deducted from the collateral.

(4) Safety Module/ Safety Incentive[104]

- 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>

i) The AAVE token holder stakes (locks) the AAVE token in the SM.

ii) A portion of AAVE's fee income is paid to the staker as compensation.

iii) 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).

iv) The funds acquired through the auction will be used to eliminate the funding shortfall.

v) 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.

*Out of the total 16 million tokens issued for AAVE tokens, 3 million tokens have been distributed for operational reserves.

[104] Aavenomics Safety Module https://docs.aave.com/aavenomics/safety-module

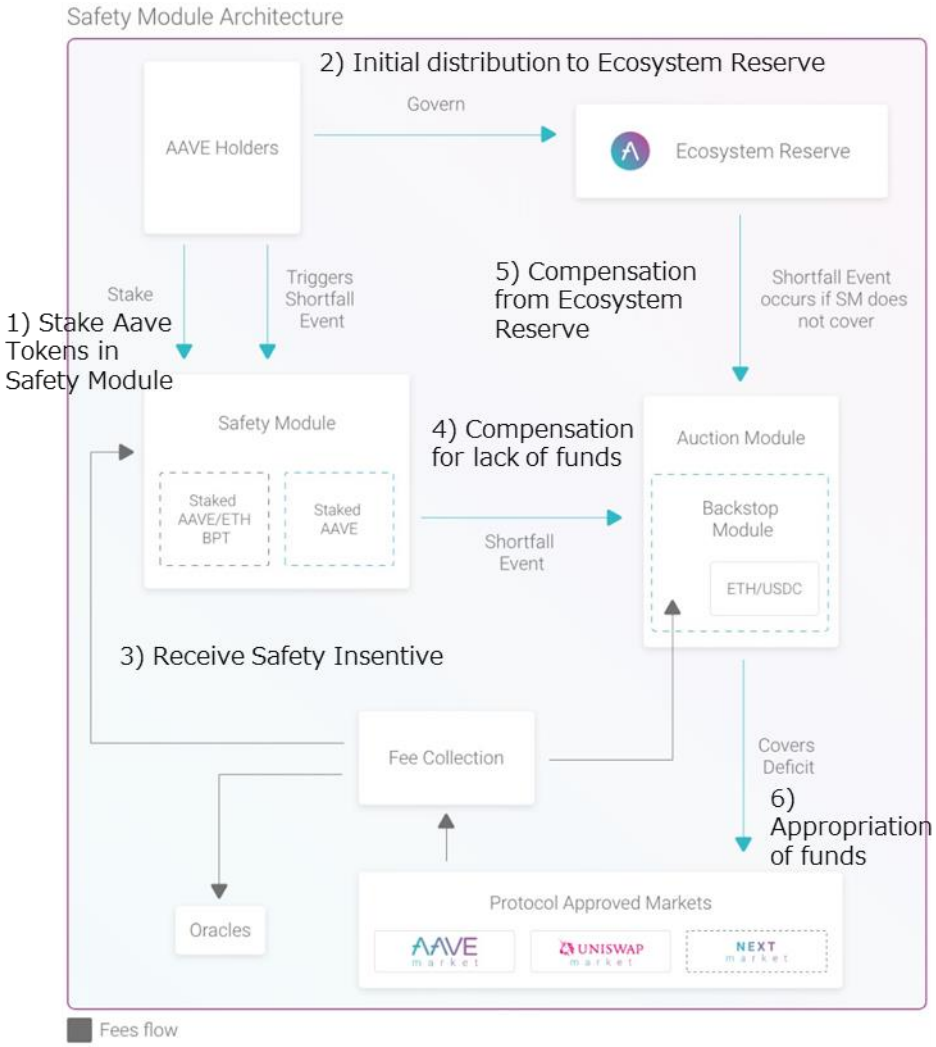


Figure 2-4-2 Aave: Safety Module / Safety Incentive

(5) Flash Loan[105]

- 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.

<Specific example of a Flash Loan (assuming arbitrage opportunities arise between the AAVE market and other exchanges)>

Execute the following ⅰ) to ⅴ) in one transaction

ⅰ) Borrow 1 ETH from the liquidity pool on an unsecured basis.

At this time, 1 ETH shall be exchangeable for 200 DAI in the Aave Market.

[105] Aave Developers Flash Loans https://docs.aave.com/developers/guides/flash-loans

ii) 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.

iii) Make a reservation to exchange 200 DAI for 1 ETH at Aave Market.

iv) Return 1 ETH and 0.0009 ETH with 0.09% commission.

v) 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)

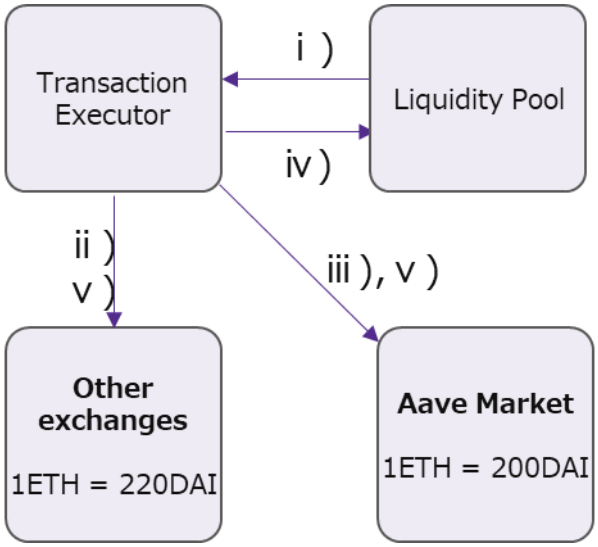


Figure 2-4-2-3 Aave: Flash Loan

(6) Credit Delegation[106]

- 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.

OpenLaw[107] : Blockchain-based electronic contracting service provided by ConsenSys.

[106] Aave Developers Credit Delegation https://docs.aave.com/developers/guides/credit-delegation

[107] OpenLaw REAL WORLD CONTRACTS FOR ETHEREUM https://www.openlaw.io/

[Example of credit delegation

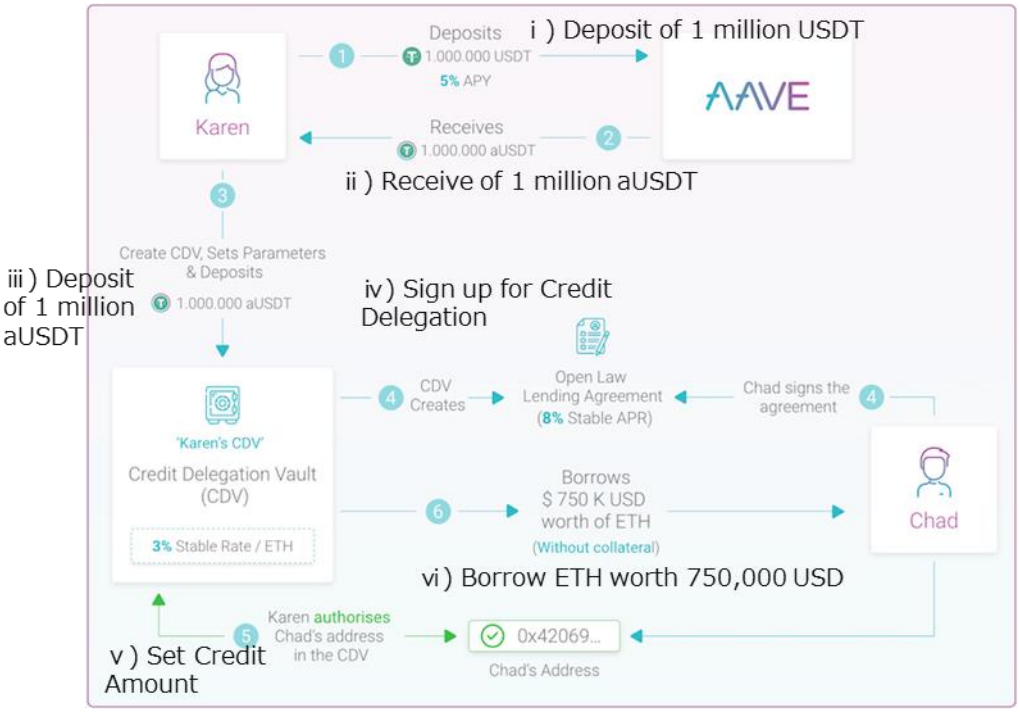


Figure 2-4-2-4 Aave: Summary of Credit Delegation

i) ii) Karen deposits 1,000,000 USDT into Aave's lending pool and obtains 1,000,000 aUSDT.

iii) Karen obtains ETH at a fixed rate of 3% by depositing 1 million aUSDT in the Credit Delegation Vault (CDV).

iv) 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)

v) After the contract is signed, Karen establishes the amount of Chad's credit according to the contract.

vi) 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.

(7) AaveArc/ Whitelister [108]

a. 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[109]

b. Whitelister

[108] Aave launches permissioned DeFi platform Aave Arc, Fireblocks becomes first whitelister https://www.theblockcrypto.com/post/129277/aave-arc-permissioned-defi-platform-fireblocks-first-whitelister

[109] Wall Street's Jane Street Borrows $25M Via DeFi Lending Platform https://thedefiant.io/jane-street-25/

- 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 to launch; Securitize (US) and SEBA Bank (Switzerland) are in the process of implementing governance proposals (as of February 2022).

<Whitelister specific example 1: FireBlock's DeFi Gateway[110] >

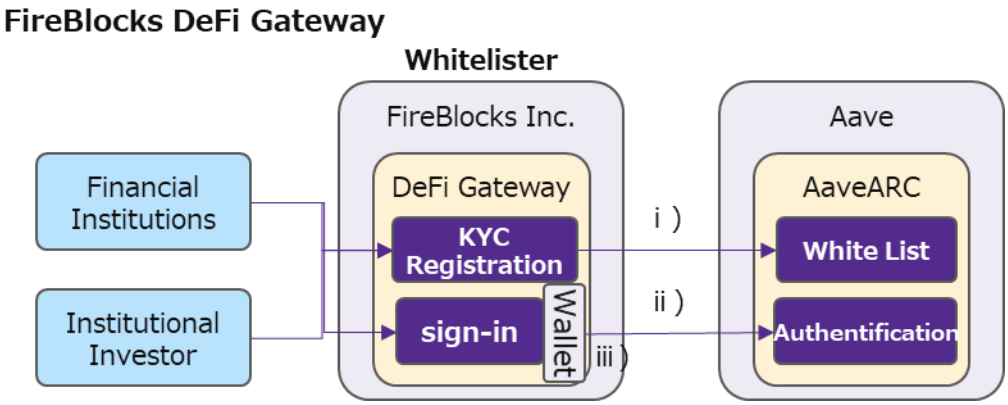


Figure 2-4-2-5-1 AaveArc Whitelister: FireBlock

Flow of authentication

i) Execute KYC with Fireblocks framework and whitelist financial institutions and institutional investors

ii) Whitelisted persons access AaveArc via Fireblocks' DeFi gateway

iii) 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.

<Whitelister Specific Example #2: Securitize, Inc. SecuritizeID[111] >

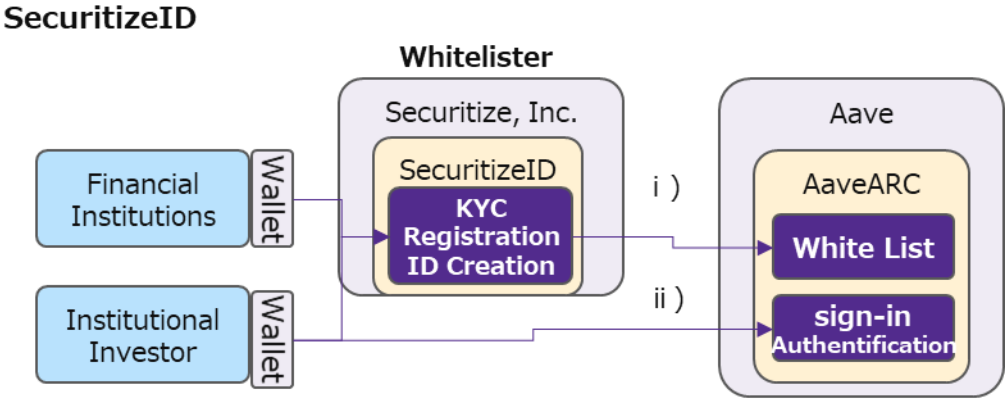


Figure 2-4-2-5-2 AaveArc Whitelister: Securitize

Flow of authentication

[110] Aave Governance Add Fireblocks as a whitelister on Aave Arc https://governance.aave.com/t/add-fireblocks-as-a-whitelister-on-aave-arc/5753

[111] Aave Governance ARC: Appoint Securitize as a Whitelister to Aave Arc https://governance.aave.com/t/arc-appoint-securitize-as-a-whitelister-to-aave-arc/6434

i) When a financial institution or institutional investor creates a SecuritizeiD in its own wallet, the wallet is linked to the AaveARC whitelist.

ii) 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.

(8) Oracle[112]

- Partnered with Chainlink, an external Oracle to obtain information on the market price of crypto-assets. Chainlink, as a decentralized Oracle, provides a service that calculates the appropriate price from multiple market prices.

(8) Scaling

Table 2-4-2-8 Aave Scaling

Item	Summary	Supplementary information
Layer 2 Solution	Aave available in multiple Layer 2 solutions - Arbitrum - zkSync - Aztec 2.0	- Platforms have restrictions on the functions that can be performed. - Different platforms have different versions deployed (e.g., V2 for Ethereum, V3 for Avalanche)
Blockchain	Aave available on multiple blockchains. - Ethereum - Avalanche - Polygon - Binance Smart Chain - Fantom - xDAI - Heco - Solana	

2-4-3 Cooperation with financial institutions

Table 2-4-3 Aave: Cooperation with Financial Institutions

Item	Summary	Supplementary information
Cooperation with Financial Institutions	- Taurus (Swiss fintech company) has formed a strategic alliance with AAVE to integrate AAVE V1 and V2 into its digital asset infrastructure, providing access to the AAVE protocol for its customers, financial institutions and institutional investors.[113] (March 2021)	Main Customers - Sygnum Bank (Switzerland) - SEBA Bank (Switzerland) - Arab Bank Switzerkland (Switzerland) - Vontobel (Swiss Investment Company)

[112] Aave Developers Price Oracle https://docs.aave.com/developers/v/2.0/the-core-protocol/price-oracle

[113] Taurus and Aave announce strategic collaboration https://blog.taurushq.com/taurus-strategic-collaboration-aave/

	- Sygnum Bank AG (Swiss digital bank) announces the launch of custody and trading services for several DeFi tokens (governance tokens) including AAVE tokens and stablecoins (USDC)[114] (June 2021)	- Tradable crypto-assets: AAVE, UNI, ANT, CRV, MKR, SNX, 1INCH
	- Launch of custody and trading services (November 2021) - Commonwealth Bank (Australia) launches 10 crypto exchanges and custody services in partnership with Gemini Exchange and Chainalysis.	- Commonwealth Bank: Established in 1911 - Tradable crypto-assets: BTC, ETH, BCH, UNI, LINK, MATIC, AAVE, COMP, LTC, FIL
	- Offer trading and custody of DeFi related products (January 2022) - Arab Bank Switzerland (Switzerland) offers 10 different crypto-asset services.	- Arab Bank Switzerland: Established in 1962 - Tradable crypto-assets: AAVE, FTM, COMP, SNX, LINK, MATIC, GRT, CRV, UNI, YFI

2-4-4 Governance operations

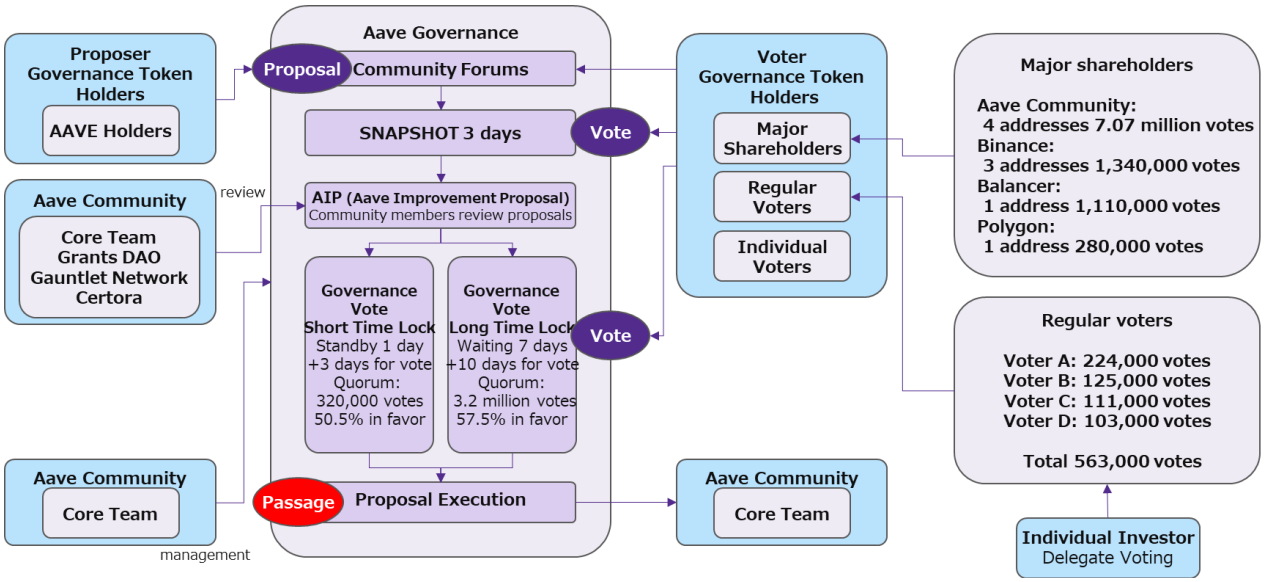


Figure 2-4-4 Governance Voting Process Using AAVE

(1) Community

Table 2-4-1 Aave: Basic Community Information

Item	Summary
Purpose of the community (summarized from official	- The Aavenomics introduce a formalized path to the decentralization and autonomy of the Aave Protocol.

[114] Sygnum launches first phase of institutional-grade access to decentralised finance
https://www.insights.sygnum.com/post/sygnum-launches-first-phase-of-institutional-grade-access-to-decentralised-finance

documentation)[115]	
Community	- Decentralized Autonomous Organizations (DAOs) by holders of governance tokens AAVE - The Core Team leads the management of the Aave community.

(2) Governance token (AAVE)

Table 2-4-2 Aave: Governance Tokens

Item	Summary	Supplementary information
AAVE Distribution	- Of the total AAVE supply of 16 million tokens - Distribution to LEND (formerly Governance Token) holders: 13 million tokens - Ecosystem Reserve funds (locked into smart contracts): 3 million tokens	- Raised $16.2 million in an ICO of LEND tokens as ETHLend in November 2017[116] - Convert LEND tokens to AAVE tokens at a 100:1 ratio for Aave v1 launch [117]
Number of addresses held by AAVE[118] (as of February 2022)	- Number of addresses held by AAVE: 100,000 - Percentage of 1st place holdings: 18.54% - Percentage of top 10 addresses held 62.30%	- Large AAVE token holders (including funds for system use) 1) Aave Protocol/ Ecosystem Reserve 4 addresses 7.07 million votes 2) Binance 3 addresses 1.34 million votes 3) Balancer 1 address 1,110,000 votes 4) Polygon 1 address 280,000 votes Of the top AAVE holders, #1-9 are protocols and crypto-asset exchanges, but voting may take place among these - In May 2021, out of 3.3 million votes in favor of the long time lock proposal, 2.7 million votes were cast by just 1 address. Based on the number of votes, it appears that the 1st place holder voted (Proposal: extend the end date of the Aave Safety Module Incentive by 100 years)
AAVE Features	1) Voting rights in on-chain voting (governance tokens) 2) AAVE protocol stabilization tool - AAVEs deposited with SM in the event of insolvency were sold at auction to compensate for losses.	-

[115] Decentralizing Aave https://docs.aave.com/aavenomics/

[116] ETHLend Token Sale event successfully Closes With $16.2 million usd raised https://medium.com/aave/ethlend-token-sale-event-successfully-closes-with-16-2-million-usd-raised-d0e0a1206141

[117] Aave Migration and Staking https://docs.aave.com/faq/migration-and-staking

[118] Etherscan Token Aave https://etherscan.io/token/0x7fc66500c84a76ad7e9c93437bfc5ac33e2ddae9#balances

	- A certain amount is retained as an AAVE reserve and used to make up for any shortfall in funds.	

(3) Decision-making

Table 2-4-3 Aave: Decision Making

Item	Summary	Supplementary information
Decision-Making Methods	- Proposals are divided into three stages of decision-making 1) Snapshot Voting See trends in favor of the proposal (temperature check) 2) AIP (Aave Improvement Proposals) Community review of proposals 3) Governance Voting AAVE holders vote to approve/reject	- Votes and proposals can be delegated
Conditions for passage of governance vote	1) Snapshot voting (off-chain) - Voting period: 3 days - Conditions for passage: Proposal must be approved by more than 50 votes for a quorum and a majority of the votes cast. 2) AIP (off-chain) - Pre-designated community members (Core Team, Grants DAO, Gauntlet Network, Certora) make the decision 3) Governance voting (on-chain) A. Short time lock Proposal: - Proposals not related to governance, such as asset lists, parameter updates, ecosystem spending, etc. - Aave Protocol, Fee collection, Contracts, AAVE Eeserve Ecosystem - Change short time lock parameters, etc. Voting period: - 1 day waiting period, 5 days grace period, 3 days voting period - Conditions for passage: - Quorum of 320,000 votes (2% of the total), 50.5% of the votes cast are in favor. B. Long time lock Proposal: - Aave Protocol Changes Affecting Governance Consensus	- 2) AIPs are not voted on, but determined by determined community members. - In 3), as a countermeasure against malicious proposals, a mechanism is in place to allow the Guardian to cancel a proposal with a 5-of-10 multisig approval during the waiting period of the governance vote.

	- Upgrade AAVE token and AAVE protocol, change governance parameters, change long time lock parameters, etc. Voting period: - 7 days waiting period, 5 days grace period, 10 days voting period - Conditions for passage: - Quorum 3.2 million votes (20% of the total), 57.5% of the votes cast are in favor.	
Actual number of votes cast (in 2021)	- Governance Vote: 46 of 53 passed (87% approval rate)	- Of the 53 governance votes, there were 2 long time lock proposals (1 passed, 1 rejected due to lack of quorum)
Items that can be proposed in the Governance Vote	1) Changes to AAVE protocol, toll collection contract, AAVE reserve ecosystem, governance parameters, and voting parameters 2) AAVE Token and AAVE Protocol Upgrade 3) Distribution of community funds (grants, compensation, etc.) 4) Guardian Recommendation	-
Aave Governance Voters (as of February 2022)	- Regular voters (same members vote on most proposals) 1) Voter A: 224,000 votes 2) Voter B: 125,000 votes 3) Voter C: 111,000 votes 4) Voter D: 103,000 votes Total 563,000 votes	- The total number of votes cast by the four regular voters exceeds the quorum of 320,000 votes for the governance proposal (short time lock) - Personal information of each voter is unknown.

(4) Addressing incidents

Table 2-4-4 Aave: Response to Incidents

Item	Summary	Supplementary information
Emergency measures to incidents	- In the event of a malicious proposal on the Governance vote, the Guardian can cancel the proposal with a multisig approval during the waiting period.[119] - In the event of an emergency, such as an external attack, Guardian can trigger an emergency key (protocol suspension) using multisig.[120]	- All multisig approvals are 5-of-10 (Ethereum blockchain).
Persons authorized to initiate	- Triggered by 10 Guardian multisignatures	- Guardian is determined by governance vote (all were most

[119] AIP 4: Activation of Aave Protocol Governance V2 https://aave.github.io/aip/AIP-4/

[120] Authorize the Guardian to hold the emergency keys for V2 https://staging.aave.com/governance/proposal/49/

emergency response		recently elected in September 2021)
Compensation for damages caused by incidents	- Damage due to incidents, etc., is the responsibility of the user and no compensation will be provided (as specified in Terms of Use[121]).	-

(5) Other

Table 2-4-5 Aave: Governance Operation and Other Matters

Item	Summary	Supplementary information
Anonymity of AAVE holders	- AAVE holders are in principle anonymous, making it difficult to identify the actual entity. - AAVE's holding addresses can be identified, but in many cases cannot be linked to real names because KYC is not performed on the majority of addresses - Institutional investors on the white list have been KYC'd and can be identified.	- Possibility of not being able to identify AAVE holders involved in decision making, making it difficult to hold them accountable

2-4-5 Aave's main trust points

(1) AAVE Limited, AAVE SAGL (affiliated corporation)

AAVE Limited, which has obtained an electronic money business license from the FCA (details of the scope of the license are unknown), and other related corporations exist.

(2) Gurdian (DAO)

A 10-member Gurdian, elected by governance vote, manages the multisig and has strong authority to cancel governance proposals and to provide emergency response in the event of an incident, etc.

(3) Venture capitalists/larger governance token holders

The reality exists that a small number of governance token holders control the majority of governance votes.

(4) External oracles

Since data on crypto-asset prices, etc. is obtained from an external oracle (Chainlink), collateral liquidation, etc. may be affected in the event of a malfunction, etc. of the external oracle.

(5) Whitelister

In order to register institutional investors on the AaveArc whitelist, certain companies accredited by AAVE conducts KYC, etc.

[121] Aave.com Terms of Use https://aave.com/term-of-use/

(6) AIP (Aave Improvement Proposal) Reviewer

Two subcontractors participate in the review of the AIP (Aave Improvement Proposal), and are considered to play a role in ensuring the reliability of the AIP.

(7) Code Auditing Company

It is assumed that users trust the results of audits by code auditing companies and use the protocol.

(8) Wallet provider

Many users use a small number of non-custodial wallets such as Metamask (not just Maker, but DeFi in general), and the impact of a vulnerability in a wallet would be significant.

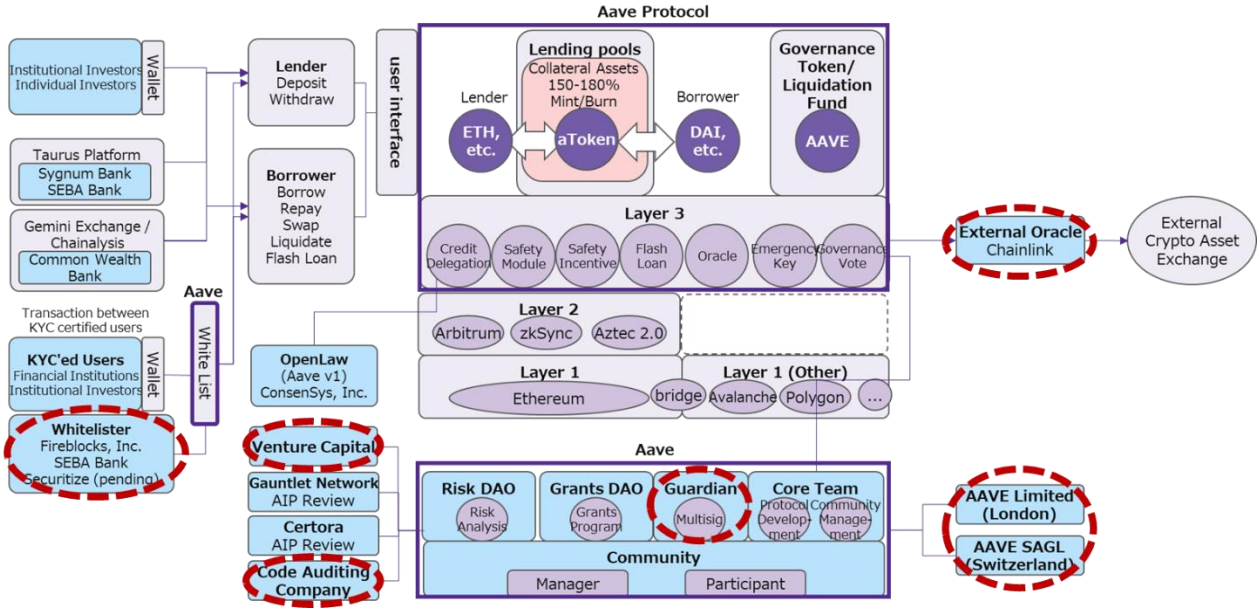


Figure 2-4-5-1 Aave's main trust points (components)

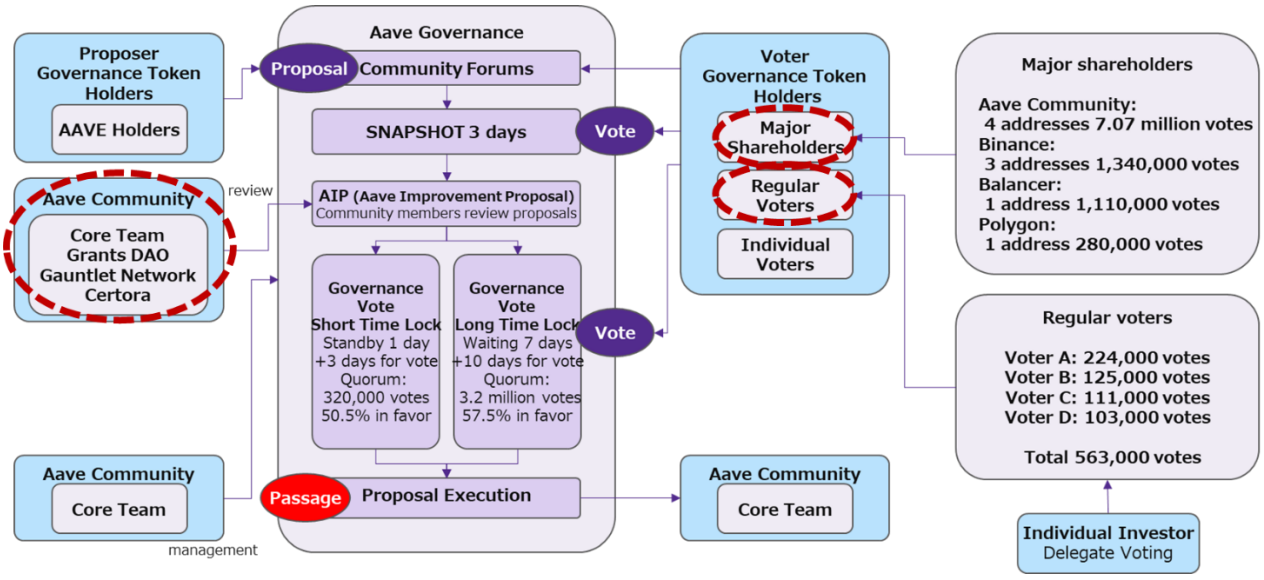


Figure 2-4-5-2 Aave's Main Trust Points (Governance Voting)

2-5 Results of Analysis of the Three Projects

We compared the three projects in terms of the organizations, their collaboration with financial institutions, technological characteristics, and governance operations to analyze trends in DeFi projects as a whole and the characteristics of individual DeFi projects.

2-5-1 Component Mapping of Major DeFi Projects

Based on the mapping results of the main components of the three projects surveyed, an example mapping of the components of the main DeFi projects with generic components is shown below. Note that the mapping example shows a basic configuration based on the major DeFI projects surveyed, and does not take into account individual requirements such as side chains consisting of specific applications.

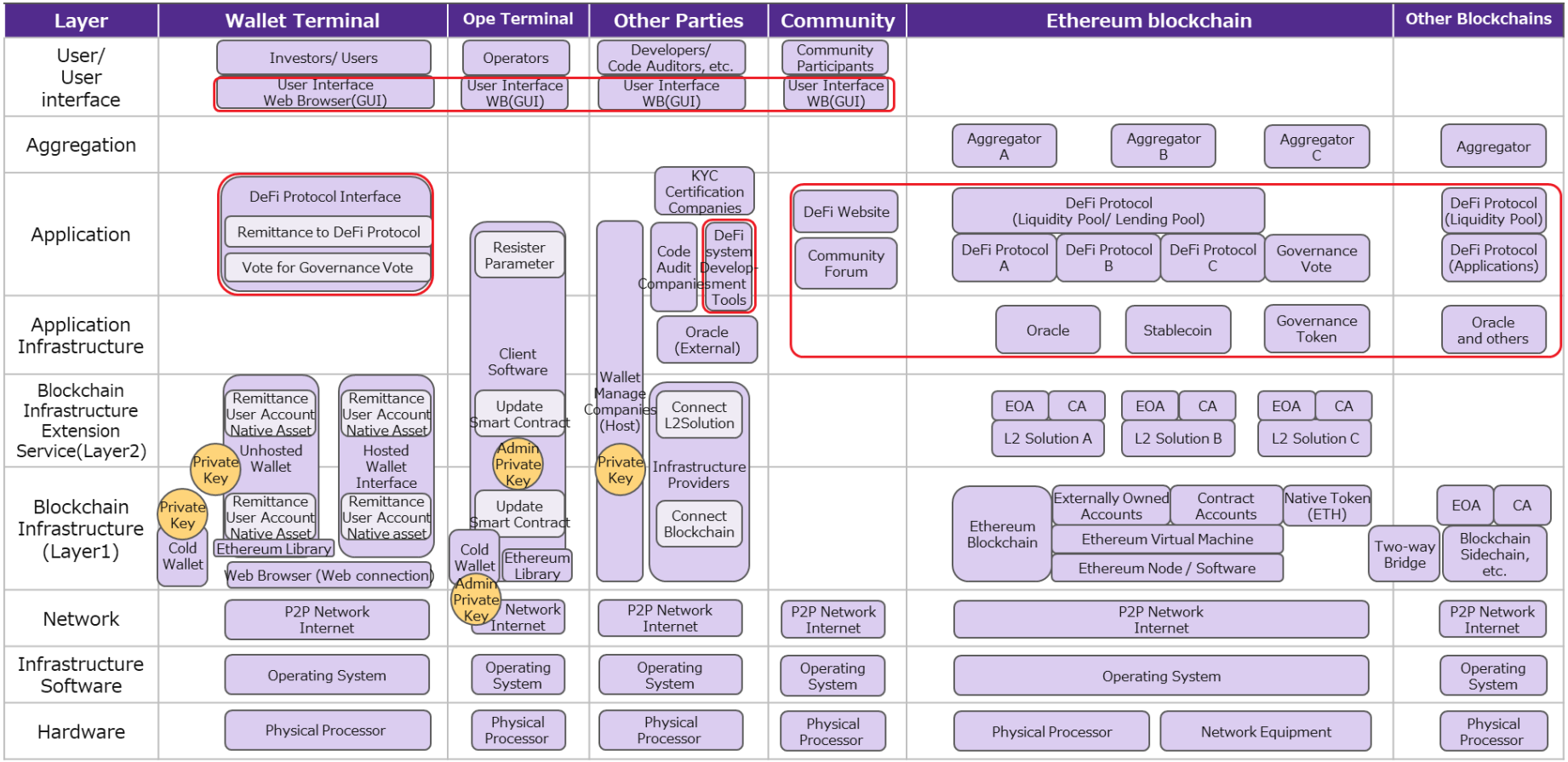


Figure 2-5-1 Mapping of Major Components of Major DeFi Projects

2-5-2 Comparison of Analysis Results for Surveyed Projects

The comparative results of the three projects studied are shown in the following table.

Table 2-5-2 Comparison of analysis results for projects studied

Item	Contents	Uniswap	maker	Aave
Summary	Services provided	Decentralized Exchange (DEX)	Stablecoin (DAI) issued	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)[122]	1.65 billion U.S. dollars - Liquidity pool fee income - UniswapV2 $827 million - UniswapV3 $817 million and others	0.69 billion U.S. dollars - Income from stabilization fees, liquidation penalties, etc.	3.1 billion dollars - Income from loan fees - Aavev2 $256 million - 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 - Involvement in certain community operations of related organizations and teams within the DAO		
		- Uniswap Labs takes the lead in protocol development and management, and interface operation and management.	- The organization within the community plays a central role in protocol development and management, and community operations. - Domain Teams: 5 teams - Core Unit: 22 teams	- The core team develops and manages protocols and community operations. - Community multisig by Guardian (outside experts approved by governance vote, 10 total) 10 members in total)
	Community Objectives (summarized from the	- UNI (governance token) is introduced for the purpose of community-led growth, development, and self-	- MakerDAO is a decentralized governance community that enables the generation of DAI,	- The Aavenomics introduce a formalized path to the decentralization and autonomy of the Aave Protocol.

[122] https://cryptofees.info/2021

	official documentation)	sustainability, enabling shared community ownership and a vibrant, diverse, and dedicated governance system. - Uniswap has always embraced the tenets of neutrality and trust minimization: it is crucial that governance is constrained to where it is strictly necessary. - Uniswap governance framework is limited to contributing to both protocol development and usage as well as development of the broader Uniswap ecosystem.	the world's leading decentralized stablecoin. - The decentralized governance community of MakerDAO manages the generation of DAI through an embedded governance mechanism within the Maker Protocol. - MKR holders have the sole authority to enact changes to the system through voting.	
	Management of community funds	- Management of wallets holding Grants Program funds - Approved by the Grant Allocation Committee with a 4-of-5 multisig out of 6 members[123]	- Management of wallets holding community funds - Four of the core unit facilitators are nominated and approved in a 2-of-3 multisig[124]	- Management of wallets holding community funds - Although not explicitly stated in the documentation, it is assumed that community members (Core Team, Grants DAO, etc.) hold the administrator's private key. - It was noted that the signer of Aave's Polygon market multisig (3-of-5) is unknown and that one Aave member may hold five private keys.No response from the Aave community. (From May 2021 DefiWatch)[125]
	Main Related Organizations	Uniswap Labs (U.S.) - Protocol development and management, involvement in community management, etc.	DAI Foundation (Denmark) - Intellectual property management, etc.	Aave Limited (U.K.) - Already licensed by FCA as an electronic money vendor Aave SAGL, Switzerland

[123] Uniswap Grants Program v0.1 https://gov.uniswap.org/t/rfc-uniswap-grants-program-v0-1/9081

[124] MIP47: MakerDAO Multisignature Wallet Management https://mips.makerdao.com/mips/details/MIP47#sentence-summary

[125] Defi Watch Aave on Polygon has an admin key https://defiwatch.net/tag/aave/

			RWA Company LLC (Cayman Islands) - Manage investments in real-world assets, sign contracts with clients, etc. Maker Ecosystem Growth Foundation (MEGF) (Cayman Islands) - Ecosystem, Oasis system (wallet, etc.) development - Information linkage with the community	- Registered as a software manufacturer
	Dissolved Organization	-	Maker Foundation (Denmark) - Upon dissolution in July 2021, Maker Foundation assets were transferred to MakerDAO and operations was taken over by domain teams/core units within MakerDAO	-
	Partner Company	-	-	Gauntlet Network (U.S.) - Participate in the review of AIP (Aave Improvement Proposals) as a risk parameter assessment contributor Certora, Israel - Participate as a security contributor in the review of the Aave Improvement Proposal (AIP) for the Aave Governance Proposal
Technical characteristics	Main Technical Characteristics	- AMM (Automated Market Maker) - Flash Swap - Concentrated Liquidity - Flexisible Fee	- Maker Vault (DAI generation) - Liquidation System 2.0 - Dai Direct Deposit Module (D3M) - Keeper (market makers/ auction) - Flash Mint	- Aave interest bearing tokens (aToken) - Flash Loan - Credit Delegation - Aave Arc/White Lister

	Oracle Functions	- Price calculation within own project without using Oracle - Calculate TWAP (time weighted average price) by taking the cumulative total of prices of crypto-asset pairs - Measure market prices for all crypto-asset pairs before any trades are made	- Oracle's structure within self-projects - Oracle Price Feed" gets prices from multiple external markets - Overall median price is calculated and reflected in the internal price after 1 hour	- Dependent on external oracle services - 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 - (AMM, liquidity aggregation functions, oracle functions, etc.) - Some parameters (fees) can be changed. - Contracts other than the core (fees, peripherals, interface, governance voting, etc.) can be changed. - It is believed that the development company has administrative privileges (administrator's private key) to modify the code.	- Smart contracts are upgradeable. - Supported by incorporating a feature in the smart contract that allows upgrades to be made in advance	
			- Domain team and core unit facilitators are considered to have administrative privileges in deploying code	- 10 Guardian multisigs approve code deployments - Was Core Team's 3-of-5 multisig management, but delegated to Aave Governance management in November 2020
	Supported Blockchains (Scalability) *Blockchains where the protocol is deployed and the token is available	- Ethereum - Ethereum 2nd Layer solution (Optimism, Arbitrum) - Side chain (Polygon)	- Ethereum - Ethereum 2nd Layer solutions (Optimism, Arbitrum, Loopring, zkSync, Aztec 2.0) - Sidechains (avalanche, Polygon, BSC, Fantom, Klaytn, xDAI, Harmony, solana, Celo, Moonriver)	- Ethereum - Ethereum 2nd Layer solution (Arbitrum, zkSync, Aztec 2.0) - Side chains (avalanche, Polygon, BSC, Fantom, xDAI, Heco, Sora)
	Emergency response	- Details unknown - The smart contract allows for proposal cancellation by the administrator, but does not define a proposal cancellation function or an administrator		- Governance proposals can be canceled

	1) Cancellation of malicious proposals	who can perform it (assuming it is performed by the developer or core unit in case of emergency?)		- 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
	Emergency response 2) Urgent smart contract fixes	- In principle, not supported because the core contract is not upgradable.	- Dark spell mechanism allows for emergency correction - A mechanism to modify smart contracts to fix critical vulnerabilities. - 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. - Content unknown as not defined in documentation (assumed to be performed by core team in case of emergency)
	Emergency response 3) What to do when attacked		- Protocol can be stopped by emergency shutdown - A certain number of governance vote protects Maker Protocol from Malicious attacks - Vote at any time, regardless of the proposal.	- Possible to pause the protocol with the emergency key - In the event of an emergency, such as an external attack, Guardian's multisig approval can trigger an emergency key.
Community Decision-Making	Number of Governance Tokens Distributed	- UNI: 1 billion tokens being distributed sequentially - (being distributed over 4 years starting in September 2020)	- MKR: 1 million tokens already distributed - (as of January 2022)	- AAVE: 16 million tokens already distributed - (as of January 2022)
	Initial Distribution of Governance Tokens 1) Free Distribution	- Initial distribution in the following percentages - Community members 60% - Team members, employees 21.266% - Investors 18.044% - Advisors 0.69%	- Distributed and sold 1 million tokens - Distribute a portion to early adopters	- Former LEND token holders 13 million tokens - Breakdown: Founder & Project 23%, Investors 77 - Reserve fund: 3 million tokens[126]

[126] https://messari.io/asset/aave/profile/launch-and-initial-token-distribution

	Initial Distribution of Governance Tokens 2) Paid Distribution	None	- Sold to venture capitalists via ICO (Andreessen Horowitz, Polychain Capital, etc.)	None
	Number of addresses holding governance tokens	276,000 addresses	83,000 addresses	106,000 addresses
	Role of Governance Tokens	1) On-chain voting	1) On-chain voting 2) Used to recapitalize stablecoin DAIs (add or delete DAIs) 3) Used as funds (MKR issued) in case of shortage of liquidation funds	1) On-chain voting 2) Used as a reserve fund (safety module) in case of insufficient liquidation funds
	Items that can be proposed in the Governance Vote 1) Application	1) Smart contract changes - Non-core application processing (additional liquidity pool changes, interfaces, governance voting, etc.) - Change parameter values (e.g., fees)	1) Smart contract changes - Application processing (D3M, Vaults, Clearing Systems, Oracle, etc.) - Change parameter values ➢ Additional changes to new collateral asset types ➢ Additional changes to existing risk parameters ➢ DAI Savings Rate Changes - Decide on system upgrades 2) Selection of oracle price feeds	1) Smart contract changes - Application processing (Lending, SM/SI, Flash Loan, Credit Delegation, etc.) - Change parameter values (e.g., commissions) - Decide on system upgrades
	Items that can be proposed in the Governance Vote 2) Governance	1) Change in community management - Distribution of community funds, changes in governance voting 2) Modification of the term of core contract commercial license, waiver	1) Change in community management - Distribution of community funds, changes in governance voting 2) Execution of emergency shutdown (always possible to vote)	1) Change in community management - Distribution of community funds, changes in governance voting 2) Guardian Recommendation
	Items that cannot be	1) Smart contract changes	(No specific restrictions)	(No specific restrictions)

	proposed in a governance vote	System upgrades (performed by the developer)		
	Governance Voting Process	Two-tier voting: snapshot voting and governance voting 1) Snapshot - Voting 2 days, quorum 0.05%, over 50% in favor 2) Governance Vote - Voting 5 days, quorum 4%, over 50% in favor	Choose between Governance Voting and Executive Voting, depending on the nature of the proposal. 1) Governance Poll - Decide on policies, etc. other than changes to the smart contract, such as the amount, interest rate, and selection of personnel, etc. - Voting 7 days, quorum 1%, 50% or more in favor 2) Executive Vote - Determine only the portion of the smart contract that is changed - Vote 30 days, quorum 1%, 50% or more in favor	Two-tier voting: snapshot voting and governance voting 1) Snapshot - 3 days to vote, quorum 50 votes, 50% or more in favor 2) Governance Vote - Short time lock (not related to governance): 3 days of voting, 2% quorum, 50.5% or more in favor - 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 - Management can cancel proposals during the waiting period. - Deployed by administrator after waiting period	- Waiting period after the proposal is approved (2 days for B only) - Authority can cancel proposals during the waiting period - After the waiting period, anyone can deploy	- Waiting period after the proposal is approved 1) 1 day 2) 7 days - During the waiting period, the selected Guardian can cancel the proposal. - Deployed by administrator after waiting period
	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) - Governance Voting 86% (6/7)	- Governance Voting 90% (275/307) - Executive Voting 100% (47/47)	- Short time lock 88% (45/51) - Long time lock 50% (1/2 case)

	Main Voters	Large token holders Mainly 10 organizations - 4 universities (Berkelay, Stanford, Harvard, UCLA) - Fintech (Gauntlet, Dharma, Kiva) - VC (Andreessen Horowitz, Monet Supply, Index Corp.) Individual investors can delegate voting rights Other voters Mainly 3 - DeFi project stakeholders (Ethrerum Foundation, Variant, Compound, etc.)	Voting proxy 18 Address - Public Agent 9 Address - Non-public Agent 9 Addresses Individual investors can delegate voting rights. Large private investor (anonymous)	Large token holders 4 addresses (including funds for system use) - Aave - Binance - Balancer - Polygon Regular voters 4 addresses (anonymous) - The 4 addresses have made decision on most of the proposals on the 1) snapshot. - Individual investors can delegate their voting rights.
Cooperation with Financial Institutions	Settlement-related	Use for debit card settlement funds - Crypto.com Payments can be made to about 30 stores such as UNI, MKR, AAVE, etc. for product purchases (Shopping.io) and travel (Travala.com)		
		-	- Monolith Convert DAI into fiat currency and load onto Visa debit card for use	-
	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). - Frankfur Stock Exchange in Germany: Euro-denominated Valour Uniswap ETP (October 2021) - 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)
	STO Real Estate Loan STO: Security Token Offering	-	- Formed partnership with Forge (digital assets subsidiary of Société Générale) for real estate loans through STO (October 2021) - *Six entities in the DAI issuance plan 1) Société Générale 2) Forge 3) MakerDAO protocol 4) Legal representative of MakerDAO 5) Role of the DIIS Group (French Fixed Income Investors) Securities Agent 6) Exchanges	-
	Other Initiatives	- The company is reportedly considering entering the market through a tie-up with a Fintech company (July 2021). - PayPal	Donate to charity (pay as USD) - UNICEF (charity organization) - NeedsList (Disaster Relief) - PoolDai (Charitable Giving Fund) Payroll Solutions	AaveARC - Ability for institutional investors who have undergone financial due diligence to borrow and lend crypto-assets with other approved institutional investors

		- Robinhood (U.S. stock management application operator) - E*Trade (U.S. online brokerage firm) - Stripe (U.S. online payment), etc.	- Whisp Money (in some communities, payroll is paid with DAI to outside employers with KYC unstable)	Whitelister - Firms approved by Aave to register institutional investors on the AaveARC White List - Registered: U.S. company Fireblocks (January 2022) - In the process of registration: Securitize (U.S.), SEBA Bank (Switzerland)

2-6 Results of Major Incident Case Analysis of Other DeFi Projects

We did research on some major incidents that occurred outside of the three projects studied. An overview of the incident, the reasons for its occurrence, and the problems and responses to them are described as below.

2-6-1 The DAO Attack

The DAO is a decentralized investment fund on Ethreum deployed by Slock.it (Germany) in April 2016 and is considered the first DAO. Participants received DAO tokens in exchange for transferring ETH to The DAO, where investment targets were voted on by the token holders and investment returns were distributed as rewards. This paper provides an overview of the June 2016 attack on The DAO that targeted the reentrancy vulnerability and the Ethereum hard fork that was implemented as a response to the attack, as well as the reasons for the attack and the issues involved.

(1) Date of Occurrence: June 17, 2016

(2) Outline of the case

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.

(3) Damage: No damage due to hard fork. Temporary damage stolen was approximately $70 million. (3.6 million ETH)

(4) Case flow[127]

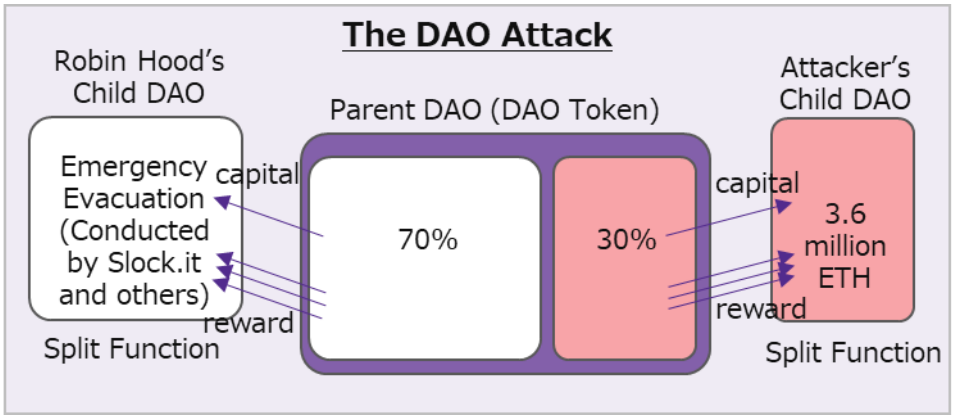


Figure 2-6-1 The DAO Attack

1. The DAO[128] Split function[129] is used to create its own child DAO independent of the parent DAO.
2. Exploiting a vulnerability in the Split function, the attecker 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

[127] SEC Report; https://www.sec.gov/litigation/investreport/34-81207.pdf
Harvard Law School Report: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3014782

[128] The DAO: an autonomous diversified investment fund established by Slock.it (Germany)

[129] Split function: A function that allows users who disagree with an investment proposal to separate their own funds from the parent DAO, the pool of investment funds, and split them into child DAOs; creation of child DAOs through the Split function requires curator approval and DAO voting approval (one week).

transferred more funds than the attacker held to the child DAO for a total of 3.6 million ETH.

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)
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.
5. The following three proposals were considered as possible solutions to the incident, and 3) Hard fork[130] was executed.

   1) Do not fork and surrender the funds to the attacker
   2) Soft fork and freeze the attacker's account
   3) Perform a hard fork and make it look as if the transaction itself never happened.
6. Opposition to the hard fork split within Ethereum, creating Ethereum Classic, which maintained the original transaction record.

Table 2-6-1-1 History of The DAO from Establishment to Incident

Date	Events	Contents	Supplement
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. - 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 - 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 - This user notified Ethereum developer and Bitcoin Foundation founder Peter Vessenes	- 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

[130] Hard fork: An update that does not guarantee backward compatibility after the fork. The rules are rewritten, resulting in a permanent fork.

		- 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	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	-
June 6, 2016	DAO Vulnerability Disclosure	- Vulnerability in The DAO Smart Contract Announced by Slock.it - 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 - 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 ➢ Griff Green, Community Manager, Slock.it, Inc. ➢ Ethereum developer Alex Van de Sander ➢ 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 1) do nothing Attackers gain 3.6 million ETH 2) soft fork The attacker's child DAO is frozen and cannot be transferred. However, 3.6 million ETH will not be returned to the investor	- 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. - Opinions in favor of hard forking ➢ Humans should make the final decision

		and will be a loss to the investor 3) hard fork - Transfer all investor funds, including the stolen 3.6 million ETH, from The DAO to a recovery address to avoid investor losses	through social consensus. ➢ It is ethically wrong for the attacker to profit and requires community intervention. ➢ Leaving ETH in the hands of an attacker could reduce its value in the future. - Opinions of opponents of hard forking ➢ The unwinding of transactions is contrary to the blockchain philosophy of "Code is Law", "Trustworthiness", and "Immutability". ➢ It undermines the original purpose of the Ethereum blockchain and makes the rules of the code base subject to human interests.
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	-

(5) Cause of Occurrence

- Phenomenal Factors

  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.

  ii) A mechanism to update smart contracts that are running was lacking.

- Motivational Factors

  Slock.it failed to recognize 2) above and failed to deploy the modified code before it was attacked.

(6) Incident Issues

Table 2-6-1-2 The DAO Attack Incident Issues

Item	Sub-Item	Description of issues	implication
Phenomenal Factors	Deployment	- Reentrancy vulnerability in the DAO reward transfer function. - Because the DAO smart contract was designed to update the internal token balance after transferring funds, a vulnerability existed that allowed	- Vulnerability attacks cause financial damage to participants

		another function to be called before the token balance was updated, allowing the funds to be transferred again without updating the token balance.	
		- Vulnerabilities in DAO source code were not discovered in advance by code audit. - The source code was reviewed by a security audit company, but the vulnerabilities were not found. - (Ref.) SEC report: "DAO's source code was reviewed by "one of the world's leading security auditing firms" and no problems were left behind during a five-day security analysis."	
		- Lack of a mechanism to update deployed smart contracts on an emergency basis - Code fixes were deployed prior to the incident, but updates required a soft fork/hard fork and could not be updated urgently at the time of the incident	- In the event of an emergency, the smart contract cannot be updated and the attack cannot be defended against.
	Governance	- The organization was aware of the vulnerability, but was not proactively taking countermeasures. - Slock.it announced prior awareness of the code vulnerability and stated that no DAO funds were at risk of the vulnerability with a workaround created, but the code for the workaround was never deployed. - Slock.it initially offered a broad security proposal, but was criticized for the high cost of this proposal and limited its countermeasures.	- The vulnerability was disclosed, but no countermeasures were taken, resulting in an attack.
Motivational Factors	Operation	- Authority was concentrated in the curator (the administrator who serves as a fail-safe function) - The curator was an individual appointed by Slock.it. - Curators could make decisions based on subjective criteria. Decisions on the adoption or rejection of investment proposals, timing, order, frequency, and halving the voting quorum (including proposals to dismiss curators), etc.	- The investment projects are decided according to the will of the founding companies and curators, and do not reflect the will of the participants. - Participants cannot effectively dismiss curators
		- DAO token voting rights were restricted. - Curators did not provide participants (DAO token holders) with sufficient information about the proposal.	- Unable to trigger improvement activities due to disadvantage of participants and have to rely on founding companies and curators

		- Participants were anonymous, making it difficult for them to unite against the curators.	
	Governance	- A soft fork/hard fork was considered as a solution to the incident, shaking the very foundations of the blockchain against its philosophy (Code is Law, reliability, immutability)	- Trade-off between blockchain philosophy and human interests (recovery from damage caused by human intervention)
		- A DeFi project incident affected the entire Ethereum platform. - The DAO was attacked, but the solution was a hard fork of the Ethereum platform - The Ethereum hard fork affected applications on Ethereum not related to The DAO.	- DeFi project glitch affects entire platform - Platform support could affect other applications
	Compliance	- No international rules have been established for incidents on global platforms - Ethereum is a global platform (Ethereum Foundation is a Swiss non-profit organization) and can only be regulated in countries where it is itself registered (not subject to every national law and regulation where it provides services). - There is no international agreement on how to investigate and respond to incidents on Ethereum.	- No legal protection for participants outside the country of registration - Global investigation and measures to incidents cannot be conducted smoothly.
		- The DAO was not registered as a stock exchange. - The DAO may have been required to register as it met the definition of a U.S. stock exchange in terms of providing a trading platform for DAO tokens.	- Concerns on Investor Protection
		- DAO token was not registered for sale. - DAO token was determined to be securities by the SEC, meaning it had be registered before sales.	- Concerns on Investor Protection

2-6-2 Flash Loan Attack #1

Here, wel provide an overview of the Flash Loan Attack incident case that occurred on bZx[131] , a margin trading and lending platform, in February 2020, the reasons for the incident, and the issues involved.

(1) Date of Occurrence: February 15, 2020

(2) Damages: approximately $350,000

(3) Summary of the Incident

By attacking a vulnerability in bZx's margin trading smart contract, the defendant intentionally

[131] https://bzx.network/

inflated the price of WBTC through the mass exchange of ETH and stole 1,271 ETH through arbitrage.

(4) Case flow[132]

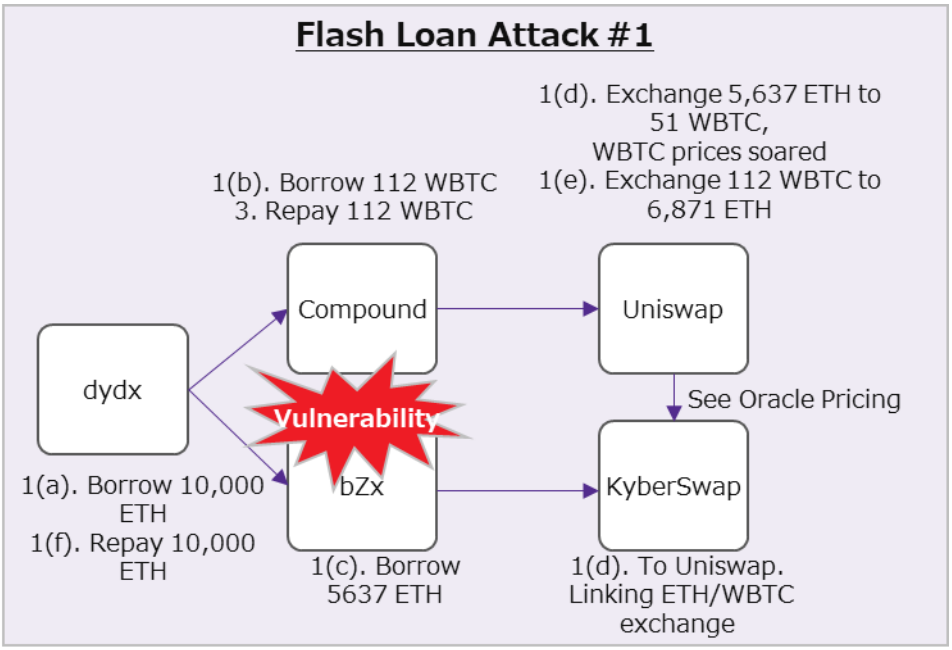


Figure 2-6-2 Flash Loan Attack #1

1. The following a) to f) were continuously executed in one transaction by Flash Loan.

   a) The attacker borrowed 10,000 ETH from dYdX[133] via Flash Loan.
   (Major DeFi's that offer the Flash Loan feature: Aave, dYdX, Equalizer, etc.)

   b) The same attacker borrowed 112 WBTC[134] from Compound[135] with 5,500 ETH as collateral.

   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)

   d) 5,637 ETH borrowed on Zx was exchanged for 51 WBTC on KyberSwap[136]
   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).
   (Uniswap's exchange rate: 38 ETH/WBTC at normal time -> soared to 109 ETH/WBTC, about 3 times the normal rate)

   e) Aiming to take advantage of the surge in WBTC prices on Uniswap, the ataccker exchanged 112 WBTC that was borrowed from Compound on Uniswap for ETH, earning 6,871 ETH.

   f) With dYdX, the 10,000 ETH borrowed from Flash Loan is repaid, resulting in a profit of 71 ETH as the difference.
   (Profit 71 ETH = 6,871 ETH exchanged + 4,200 ETH unused - 10,000 ETH repaid)

---

[132] https://peckshield.medium.com/bzx-hack-full-disclosure-with-detailed-profit-analysis-e6b1fa9b18fc
https://bzx.network/pdfs/CertiK_Review_Report_for_bZx_v2.pdf

[133] dYdX: DeFi platform for margin and derivatives trading: https://dydx.exchange/

[134] WBTC: Wrapped BTC Stablecoin linked to Bitcoin on Ethereum

[135] Compound: lending platform with TVL second to AAVE: https://compound.finance/

[136] Kyberswap: DeFi platform for decentralized exchanges: https://kyberswap.com/about/kyberswap

2. WBTC price then returned to normal, at 38 ETH/WBTC.
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.

(5) Cause of Occurrence

- Due to an attack that exploited a vulnerability in bZx's margin trading smart contract.
- 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.

Table 2-6-2: Flash Loan Attack #1 Incident Issues

Item	Sub-Item	Description of issues	Existing Risks
Phenomenal Factors	Deployment	- Vulnerability in bZx's margin trading smart contract. - bZx margin trading intentionally inflated WBTC prices due to vulnerability of positions not being liquidated due to lack of ETH collateral - After the incident occurred on February 15, the system was temporarily shut down and a smart contract upgrade was announced on 2/16 (the fix was completed on February 17)	- Vulnerability attacks cause financial damage to participants. - The spread of damage caused by the attack will reduce confidence and investment in the crypto-asset itself. - If there are too many attacks, the overall confidence in the DeFi market will decrease.
		- Failed to discover vulnerabilities in bZx source code in advance - Source code was reviewed by a code auditing company, but no vulnerabilities were found. - The audit was conducted by CertiK on February 2020 and noted 6 points of improvement information, although there were no serious vulnerabilities. However, the vulnerability that caused this issue was not detected	
Motivational Factors	Deployment	- There are two ways to deploy: voting and emergency, which presents challenges for management. - In normal times, the governance tokens vote to approve, but fixes for non-urgent vulnerabilities are included in regular updates and take longer time to address (vulnerability fixes should not be voted on). - In an emergency, deployments can be made without a vote, creating loopholes such as developer intentionality.	- Participants' losses due to attacks prior to fixing vulnerability responses in periodic updates. - Decrease in confidence in applicable crypto-assets
	Governance	- Governance was managed by voting with governance token (BZRX), but in reality it was managed by the core	- Participants are harmed by intentional proposals

		founders and team members of the founding company, bZeroX, LLC, and decision-making authority was centralized (No specific relationship between this incident and governance issues)	by founding companies, core founders, etc.

*Revised bZx Governance Rule to address governance issues (effective since August 2021)[137]

- Process to approve proposals by vote of governance token (BZRX)
  Stage 1: Forum Discussion
  Submit proposals for review
  0.5% of the total (5.15 million BZRX) consent required (2 days)
  Stage 2: Snapshot Voting
  Requires a minimum of 50% approval + 4% of the total (41.2 million BZRX) consent (3 days)
  Stage 3: On-chain governance decisions
  Proposal will be implemented after TimeLock (2 days) Minimum 7 days total
- Items to suggest
  Funding, fees, token related, ecosystem related, marketing, development roadmap/feature prioritization, salaries and personnel movement

2-6-3 Flash Loan Attack #2

The Flash Loan Attack incident case that occurred again in bZx immediately after the 2-6-2 incident in February 2020 is discussed here, with an overview of the incident, the reasons for its occurrence, and the issues involved.

(1) Date of Occurrence: February 18, 2020

(2) Amount of loss: $633,000 (2,378 ETH)

(3) Summary of Incident
By attacking the Oracle vulnerability in bZx, the attacker intentionally inflated the sUSD[138] price by mass exchange of ETH and stole 2,378 ETH through arbitrage.

(4) Case flow[139]

[137] https://bzx.network/blog/bzx-dao
https://bzx.network/pdfs/CertiK%20Verification%20Report%20for%20bZx.pdf

[138] sUSD: Synthetix crypto-asset

[139] https://peckshield.medium.com/bzx-hack-ii-full-disclosure-with-detailed-profit-analysis-8126eecc1360

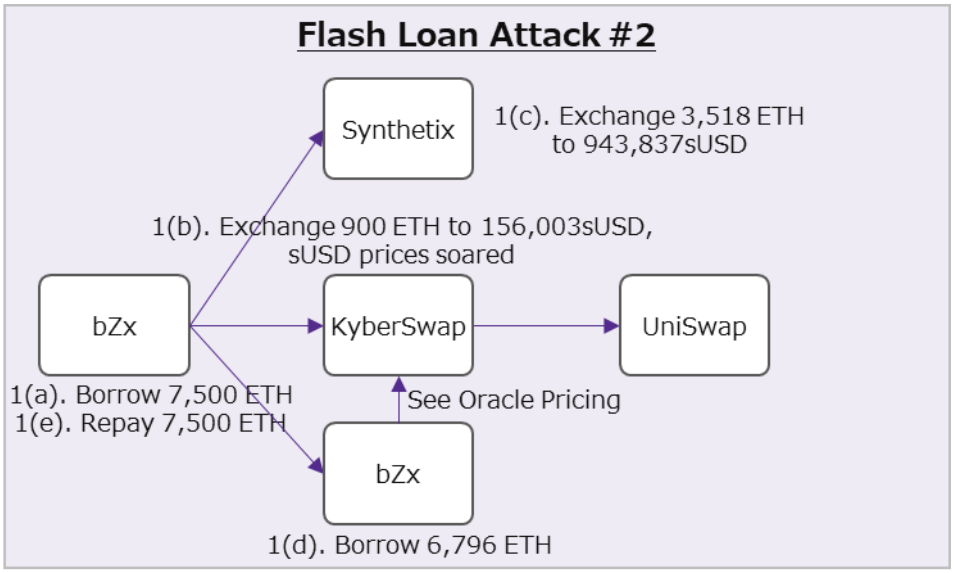


Figure 2-6-3 Flash Loan Attack #2

1. The following a) to e) were continuously executed in one transaction by Flash Loan.

   a) The attacker borrowed 7,500 ETH from bZx with a Flash Loan.

   b) Exchanged 540 ETH for 92,419sUSD on KyberSwap. Then 360 ETH was exchanged for 63,584sUSD. (Exchanged 900ETH for 156,003sUSD in total)
   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.
   KyberSwap's exchange rate: 0.00372 ETH/sUSD under normal conditions -> soared about 3 times to 0.00899 ETH/sUSD.

   c) At Synthetix[140] , 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)

   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)

   e) The 7,500 ETH borrowed from bZx was repaid and a profit of 2,378 ETH was earned. (Profit 2,378 ETH = 6,796 ETH borrowed + 3,082 ETH unused - 7,500 ETH repaid)

(5) Cause of Occurrence

- 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.

Table 2-6-3 Flash Loan Attack #2 Incident Issues

Item	Sub-Item	Description of issues	Existing Risks
Phenomenal Factors	Deployment	- Vulnerability in Oracle reference in bZx. - bZx's reliance on KyberSwap for Oracle price references caused	- Vulnerability attacks cause financial damage to participants

[140] Synthetix: DeFi project of a decentralized exchange

		KyberSwap to deliberately inflate the price of sUSD, which was targeted when the difference from the normal price increased. - Oracle reference vulnerability in bZx not discovered in advance - Source code was reviewed by a code auditing company, but no vulnerabilities were found. - CertiK's audit in February 2020 did not detect the vulnerability that caused this	- The spread of damage caused by the attack will reduce confidence and investment in the crypto-asset in question. - If there are too many attacks, the overall confidence in the DeFi market will decrease.
Motivational Factors	-	Same as 2-6-2 Flash Loan Attack #1	-

2-6-4 Money Laundering

The following is an overview of the money laundering incident case that occurred in September 2020, the reasons for the incident, and the issues involved.

(1) Date of Occurrence: September 26, 2020

(2) Damages: Approximately $275 million

(3) Outline of the case

- Approximately $275 million worth of crypto-assets were stolen from KuCoin[141], a Singapore-based crypto-asset exchange, when the hot wallet private keys of the exchange's administrators were stolen.
- The funds were dispersed and transferred to over 200 Bitcoin, Ethereum, and other blockchain exchanges.
- According to an investigation by Chainalysis, a blockchain analysis company, the attack was carried out by the Lazarus Group, a North Korean cybercrime group.
- In November of the same year, the $204 million was recovered through the freezing of assets by various exchanges and with the cooperation of the police, and almost all of the damage was covered, including compensation through insurance.

(4) Case flow[142]

[141] KuCoin: Hong Kong's Crypto-asset Exchange

[142] https://www.kucoin.com/news/en-kucoin-ceo-livestream-recap-latest-updates-about-security-incident
https://www.kucoin.com/news/en-kucoin-ceo-livestream-recap-latest-updates-about-security-incident-0930
https://www.kucoin.com/news/en-the-latest-updates-about-the-kucoin-security-incident
https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap-japanese
https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack-japan

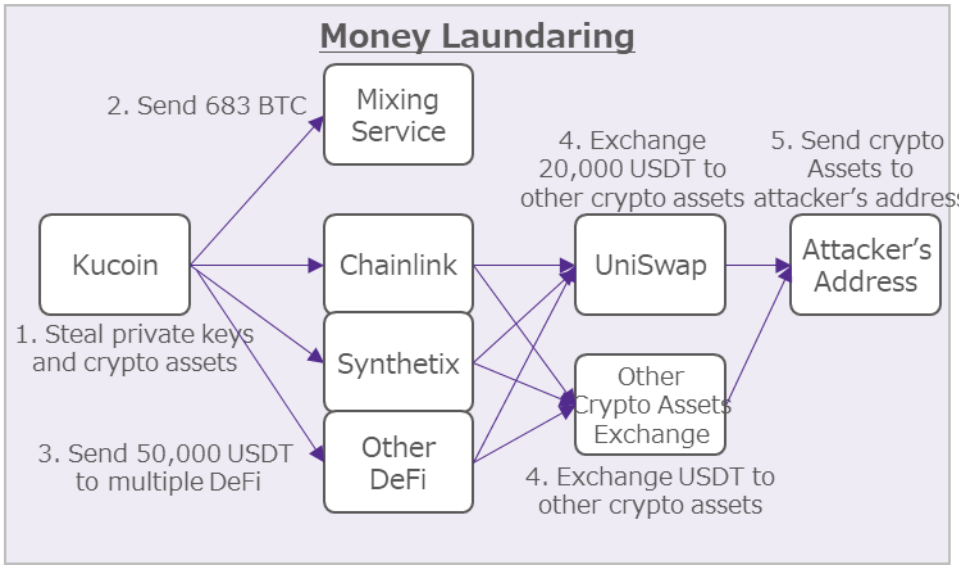


Figure 2-6-4 Money Laundering

1. An attacker stole the KuCoin administrator's hot wallet private key and a large amount of crypto-assets were stolen.
2. Bitcoin: 683 BTC of the 1,008 BTC stolen were transferred to the mixing service[143] and anonymized.
3. USDT: Of the 19.83 million USDT stolen, 50,000 USDT was transferred to Chainlink[144] , Synthetix and several other DeFi.
4. USDT: USDT transferred to Uniswap and other exchanges and converted to other currencies.
5. USDT: After redemption, the money was transferred to the attacker's address.

<Major crypto-assets leaked from Kucoin>
- 19.83 million USDT
- 1,008 BTC ($10.76 million)
- Various ERC-20*6 tokens worth $147 million (excluding USDT)
- Stellar*7 tokens worth $87 million, etc.

(5) Cause of Occurrence

- The private key of the KuCoin administrator's hot wallet was stolen. However, detailed information on the incident, including the circumstances of the theft of the administrator's private key, has not been released at this time. (It has been announced that this information would be released as soon as the investigation by the police and security authorities is completed.)
- Assets in cold wallets have not been leaked.

Table 2-6-4 Money Laundaring Incident Issues

Item	Sub-Item	Description of issues	Existing Risks
	Operation	- Stolen crypto-assets were replaced without incident.	- Stolen crypto-assets can be easily laundered.

[143] Mixing services: a method of mixing multiple Bitcoin remittance data to protect the privacy and anonymity of users. Makes it difficult to track where assets were sent from and to where.
[144] Chainlink: a decentralaized Oracle network connecting on-chain and off-chain

Phenomenal Factors		- Of the USDT stolen, 20,000 USDT was immediately converted to ETH via Uniswap	
		- It took a long time to freeze the stolen crypto-assets (no fund transfers). - Crypto-asset freezes were implemented with the cooperation of many exchanges and others to which money was transferred (each exchange handled asset freezes individually)	- The damage to stolen crypto-assets is unstoppable and escalating.
		- Attacker cannot be identified. - Stolen crypto-assets are transferred to a number of DeFi, and the attackers' destinations and addresses are recorded on the blockchain, but it is impossible to identify who did it because they use an exchange that does not require KYC	- Funds transfers can be repeated without identifying the attacker.
		- Stolen assets are difficult to trace. - Bitcoin uses a mixing service to anonymize the funds, making it difficult to identify the movement of funds after that.	- Funds transfers make it impossible to locate stolen crypto-assets
	Operation	- KuCoin administrator's hot wallet private key stolen - However, detailed information on the incident, including the circumstances surrounding the theft of the administrator's private key, has not been released at this time	- Theft of an administrator's private key results in the loss of crypto-assets and damage to participants. - Decrease in confidence in applicable crypto-assets
Motivational Factors	Technology	- Lack of technology to manage the administrator's private key - The technology required to manage the administrator's private key may not have been used (details are undisclosed and not publicly available)	- Theft of administrator's private keys through weak technology
	Operation	- The administrator did not maintain strict control of the private key. - Assumed that the administrator had a weak awareness of the importance of managing private keys.	- Private key theft due to careless management by administrators
	Governance	- Inadequate protection against theft of the administrator's private keys - Although the cause of the administrator's private key theft has not yet been announced and details are not available, it is believed that effective anti-theft measures were necessary if private key management operations were to be compromised	- Decrease in confidence in applicable crypto-assets
	Regulation	- Guidance may have been needed regarding the administrator's measures to prevent private key theft.	- Decline in trust in the DeFi market as a whole due to a number of incidents of private key

		- The detailed cause of the administrator's private key theft is unknown, but if there is a problem with the private key management operation, it is considered necessary to establish certain standards as an anti-theft measure	theft by similar administrators.

2-6-5 Bitcoin Vulnerability (CVE-2018-17144)[145]

This section provides an overview of the September 2018 Bitcoin vulnerability incident case, the reasons for its occurrence, and the issues of this incident.

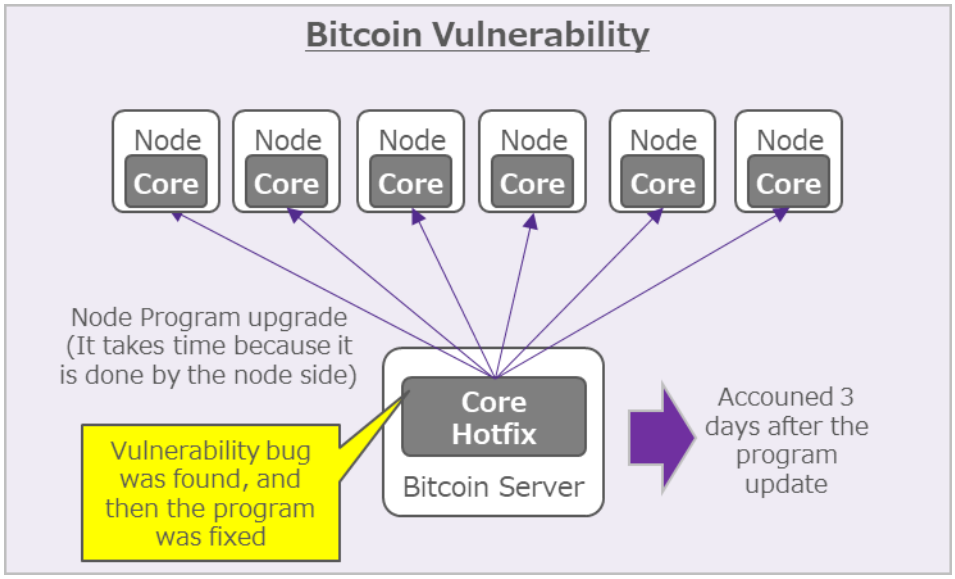
(1) Date of Occurrence: September 18, 2018

(2) Amount of loss: None

(3) Outline of the case

- For Bitcoin Core[146] versions 0.15.x, 0.16.0, 0.16.1, 0.16.2, and 0.16.2
- Vulnerabilities related to DoS attacks[147] and double payments were discovered and fixed in versions 0.16.3 and 0.17.0rc4.
- It was possible to intentionally crash the Bitcoin network node[148]by exploiting this vulnerability, and if the majority of nodes in the hash rate did not have the modified program applied, they were at risk of a 51% attack or other attacks. Therefore, the public announcement of the vulnerability was delayed to allow time for the majority of nodes to upgrade.

(4) Case flow[149]



[145] CVE-2018-17144: Common Vulnerabilities and Exposures, identifier numbered by MITRE, a US non-profit organization

[146] Bitcoin Core: An open source program that serves as the reference software for Bitcoin mining and trading.

[147] Dos Attack: Denial of Service Attack, a cyber attack that maliciously sends large amounts of data to a server to make it virtually impossible to run a service.

[148] Node: a device that processes the blockchain. Nodes have the following functions: routing, blockchain database, mining, and wallet.

[149] https://bitcoincore.org/notice/
https://hackernoon.com/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362

Figure 2-6-5 Bitcoin Vulnerability

September 17 14:57 Anonymous person discovered the vulnerability and reported it to several parties at Bitcoin Core.

September 17 17:47 Bitcoin Core developer confirms vulnerability.

September 18 20:44 Bitcoin Core developer releases fixed program.

September 18 21:47 Public banners on Reddit and other sites encouraging node upgrades.

September 19 14:06 Additional message on mailing list to encourage node upgrades.

September 20 Full disclosure of this vulnerability.

(5) Cause of Occurrence

Table 2-6-5 Bitcoin Vulnerability Incident Issues

Item	Sub-Item	Description of issues	Risks/Implications
Phenomenal Factors	Deployment	- Cases of double input of UTXO (unspent transaction output) sometimes slipped through the transaction validity check.	
Motivational Factors	Deployment	- While optimization of transaction validity checks and UTXO management has continued, the vulnerability was the result of loosening checks for further optimization in fixing of the version 0.15 fix.	- Risk of system shutdown or theft of funds
		- The vulnerability required a fix to be applied to the majority of nodes at the hash rate, which took a long time to address.	- Risk of attack by a node that does not adopt the correction program in time - If a similar vulnerability is discovered in the DAO, Responsible Disclosure may not be able to delay the announcement of the vulnerability when a program fix needs to be voted on and approved, and the public may become aware of the urgent vulnerability.
		- Node upgrades are done at the discretion of the node side, so there is no guarantee that a request to reflect a modified program will be responded to. - Malicious nodes may not update with old programs	- Nodes are not upgraded with old programs and vulnerabilities are not fixed
		- Vulnerability was inherent from Bitcoin Core version 0.15.x, but was undetected for a long period of time. - In this case, the vulnerability was discovered by an anonymous reporter.	- In this case, the anonymous person reported the vulnerability to the Bitcoin Core

			development team without disclosing it publicly, but it was up to the person to decide whether or not to disclose the vulnerability.

2-6-6 Stealing of Funds Locked in a two-way Bridge in a Side Chain (Ronin Network)

This section provides an overview of the incident case of theft of funds locked in a two-way bridge of a side chain that occurred in March 2022, the reason for the incident, and the problem. The cause of this incident was the theft of private keys of validators. 9 validators were managed by 2 companies, and 5 validators' private keys were stolen at the same time by one company's system attack, which is an unfavorable example of private key management.

(1) Date of Occurrence: March 23, 2022

(2) Losses: Approximately $620.1 million *Highest amount at the time of occurrence

(3) Outline of the case

- On March 23, the private keys of some validators of the Ronin Network[150] running Axie Infinity[151] were stolen, and the funds for the two-way bridge connecting the Ethereum network and the Ronin Network (Ronin Bridge[152]) were stolen.
- March 29, the incident was discovered when a user was unable to withdraw funds from Ronin Bridge. Sky Mavis, the operator company in Vietnum of Ronin Bridge, shut down Roni Bridge and investigated the cause.
- April 6, Sky Mavis raises $150 million from several VC firms to cover losses.
- 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.
- As of April 20, Ronin Bridge is out of service.

(4) Case flow[153]

[150] Ronin Network: an Ethereum sidechain (creating a blockchain different from the parent mainchain and transferring funds via a two-way bridge), launched in February 2021 by operator Sky Mavis exclusively for Axie Infinity.

[151] Axie Infinity: Online game where players collect, train, and compete with NFT pets 8.3 million players (as of December 2021)

[152] Ronin Bridge: a bridge that transfers funds between the Ethereum Network and the Ronin Network. Prevents double use of Ethereum coins in the parent chain by locking them into the bridge.

[153] https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r
https://medium.com/uno-re/biggest-crypto-hack-of-all-time-a-breakdown-of-the-ronin-network-hack-ef8d9e25ba6b
https://www.nansen.ai/research/ronin-the-engine-powering-axie-infinitys-growth

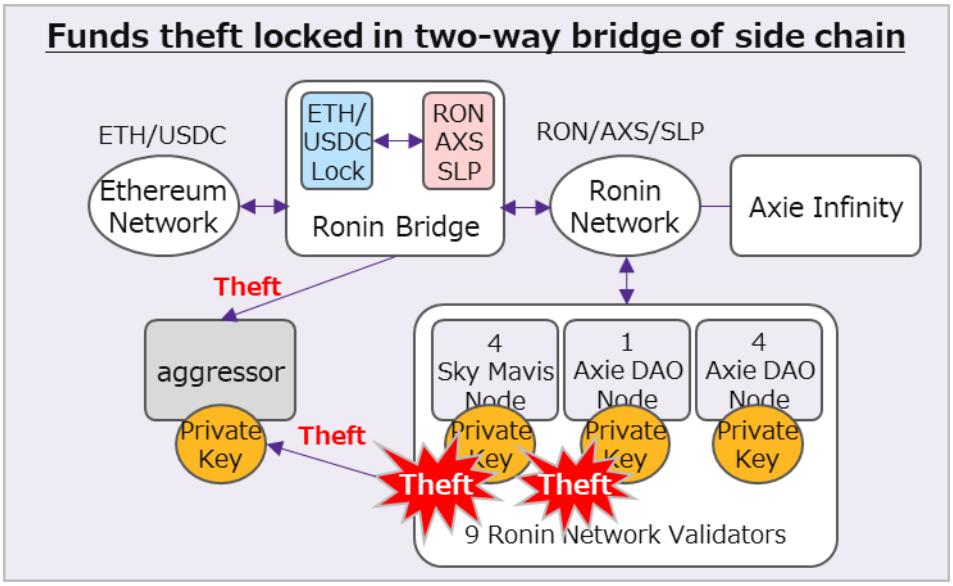


Figure 2-6-6 Outline of the case

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.)
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.
3. 3/31 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.

<Stolen Funds and Crypto-assets>
Total $620.1 million
- ETH 173,600 ETH ($594.6 million)
- USDC $25.5 million

(5) Cause of Occurrence

The cause was that the private keys of 5 of 9 nodes of the Ronin Network Validator were stolen.

- Sky Mavis 4 nodes

  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).

- Axie DAO 1 node

  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.

- 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.

Table 2-6-6: Issues with theft of funds locked to a two-way bridge in a side chain

Item	Sub-Item	Description of issues	risk implication

Phenomenal Factors	Operation	- Sky Mavis systems were attacked and the private keys of four validator nodes were stolen. (Details of the attack have not been released.)	- Theft of private keys of validators leads to theft of funds - Hijacking of validators could be used for other attacks, such as malicious contract execution
		- The private keys of four Sky Mavis validator nodes were stored on a centralized server, and the above attack resulted in the simultaneous theft of the private keys of all four validators.	- Including the private keys of the Axie DAO validators, virtually majority of the private keys were stolen in a single attack.
		- The private keys for the Axie DAO validators, which were managed separately from the four Sky Mavis validators, were also stolen at the same time.	- The attack on Sky Mavis would likely have resulted in the automatic theft of Axie DAO's private keys, and the private keys were essentially not managed separately.
Motivational Factors	Operation	- Nine private keys are managed by two organizations, Sky Mavis and Axie DAO (Sky Mavis has centralized control of the nodes. - The validator for Ronin Network may have been specified by the operator, Sky Mavis.	- When validator nodes are operated by a small number of organizations, there is an increased risk that the private keys of the validators for the number of nodes needed to make block decisions can be stolen, for example, if the private keys of the validators are stolen at the same time.
		- The PoA consensus validator threshold for the Ronin Network was "5" (5 out of 9 for a block decision). - Ronin Network is a blockchain dedicated to Axie Infinity games, and the block creation time is only about 3 seconds, which was the minimum threshold to minimize the PoA time.	- Smaller thresholds increase the risk of private key theft for validators with the number of nodes needed to make block decisions.
	Deployment	- Sidechains, such as Ronin Network, lock Ethereum funds into a bridge and convert them to sidechain crypto-assets, which locks a large amount of funds into the bridge and makes this bridge vulnerable to attackers.	- Sidechains with large transaction amounts have large amounts of money locked up in their bridges, making them easy targets for attackers. - Reference ➢ Solana blockchain on 2/22/2022 was attacked by the Wormhole bridge

			was attacked, causing $325 million in damage (due to an attack on a vulnerability in the signature contract). - Other side chains have also locked up large amounts of money in the bridge.[154] ➢ Polygon: approx. 5.51 billion dollars ➢ Avalanche approx. 4.97 billion dollars, etc. (as of 4/12/2022)
	Governance	- The attack prevented Axie Infinity players who had exchanged Ethereum ETH or USDC for Ronin RON, AXS, or SLP from being able to pay out ETH or USDC.	- Funds are not refundable. - In this case, Sky Mavis announced on 4/6 that it has raised $150 million in funding from multiple VC firms to ensure that all affected users receive refunds.

2-6-7 Major Incident Cases after 2020[155]

Many incidents have occurred due to software vulnerabilities and inadequate management of private keys.

Table 2-6-7 Major Incident Cases after 2020

Date of Occurrence	Cause	Related DeFi	Amount of damage	Case Summary
4/19/2020	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. - The attackers had trouble cashing in the stolen crypto-assets (ETH, etc.) and most of them were returned.
8/25/2020	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 - 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.

[154] https://dune.xyz/eliasimos/Bridge-Away-(from-Ethereum)

[155] https://hacked.slowmist.io/en/

				- The management team then bailed out the funds locked in the staking pool.[156]
9/14/2020	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. - Later, they found the attacker and recovered the full amount.
10/26/2020	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 - The attackers used the Ethereum mixing platform "Tornado.cash" to conceal the funds transfer. - Attackers returned $2.5 million to the developer at USDT and USDC.
11/30/2020	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.
5/18/2021	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. - 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. - 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.
8/10/2021	Software vulnerabilities (Blockch	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-

[156] https://valuedefi.medium.com/yfv-update-staking-pool-exploit-713cb353ff7d

	ain-to-blockchain transaction glitches)			assets and transferring them to multiple accounts including Binance Smart Chain, Ethereum, and Polygon. - 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.
10/27/2021	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. - This was Cream Finance's third flash loan hit, following two in February and one in August.
10/30/2021	Inadequate management of private keys	BoyX High Speed (BXH) (DEX)	US$139 million	- Private Key Compromise Leads to $139 Million Outflow - The attacker may have hacked into the private keyholder's computer or was one of BXH's technical staff
11/5/2021	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 - bZx DAO voted to approve plan for full compensation for damages
11/30/2021	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.
12/2/2021	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. - The user's address was stolen by the criminal and the funds were stolen by the user clicking on the UI.
12/3/2021	Software vulnerabilities (Token tampering)	Polygon (side chain)	US$2 million	- On 12/3, a white-hat hacker notified Polygon of a critical vulnerability (allowing an attacker to arbitrarily generate tokens using Polygon's contracts), and a patch was released on 12/5, but MATIC coins equivalent to $2 million were stolen as until the patch was apllied. - Responsible disclosure delayed the vulnerability announcement, and the fix was officially disclosed the fix on December 29.
2/2/2022	Software vulnerabilities	Wormhole (two-way bridge)	US$320 million	- A vulnerability in the smart contract (a flaw in the contract that verifies

	(Defects in the signature verification process)			signatures) was exploited, and funds locked in the bridge were stolen. - Wormhole's parent company, JumpCrypto, covered the damage with its own funds to support the Solana ecosystem.
4/17/2022	Software vulnerabilities (Inadequate emergency commit conditions)	Beanstalk (stablecoin)	US$182	- Governance voting smart contract vulnerability exploited and funds stolen by Flash Loan[157] - Incident Flow 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). 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. 2) On the day of the incident, Flash Loan performed the following on Aave ➢ Borrowed a total of $1 billion from Aave in ETH, USDC, and USDT ➢ Borrowed funds to purchase 2/3 of Beanstalk's governor tokens ➢ Vote for malicious proposals with purchased governance tokens ➢ Successfully executed a malicious smart contract by activating Beanstalk's Emergency Commit and stole Beanstalk's funds - Cause of the incident 1) No one in the community noticed the malicious proposal. - Verification of proposals depended on the cooperation of community members, and no one was able to find a malicious proposal 2) There was no mechanism to cancel malicious proposals in the Emergency Commit. - There needed to be a mechanism to cancel proposals and a cancellation period. 3) Inadequate conditions for activation of Emergency Commit in Beanstalk

[157] Beanstalk Farms loses $182M in DeFi governance exploit
https://cointelegraph.com/news/beanstalk-farms-loses-182m-in-defi-governance-exploit

				- (Activation condition) 1 day after proposal & 2/3 or more affirmative votes to be executed - 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. 4) Aave's Flash Loan was abused. - Aave's Flash Loan was exploited to attack other DeFi projects because of its unsecured, unlimited borrowing
5/10/2022	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[158] . There have been two previous occasions when the price was temporarily unable to maintain 1USD, but this time the price was unable to return. - Case Flow 1) May 5, The overall price of crypto-assets, including Bitcoin and ETH, fell. (Bitcoin fell up to 32% on 5/12) 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) 3) May 8, UST was sold for $258 million, further lowering the price. 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 5/8) - 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. - Total LUNA supply: approx. 730 million tokens as of 5/5 →

[158] Terra USD (UST) Dipeg fray: https://coinpost.jp/?p=350288

				increased to 6.5 trillion tokens as of 5/13 (approx. 8,900x) 5) May 13, Terra blockchain operations were temporarily suspended. - Market price UST: $1.0 to $0.17 (down 83%); LUNA: $80 to $0.02 (down 99%) *Anchor Protocol: a savings protocol for the Terra blockchain that offers up to 19.5% yield when depositing UST tokens. - 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)

2-7 Analysis of Trust Point Weakest Link in Chains of trust

Based on the results of the mapping of key components in the chains of trust and the analysis of major DeFi projects and major incident cases, the following are considered trust points and weakest links.

2-7-1 Analysis of Trust Points

(1) Ethereum Library[159]

- 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.
- Figure 2-7-1 Unhosted Wallet and client software depend on the Ethereum Library, and the Ethereum Library is considered a trust point

(2) Ethereum Node Software[160]

- 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).
- The Ethereum node users and miners in Figure 2-7-1 depend on the software of the Ethereum node and Ethereum Virtual Machine, and these software are considered to be trust points.

(3) 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 behaves correctly.
- Wallet terminals and operational servers in Figure 2-7-1 depend on infrastructure providers, and infrastructure providers are considered to be trust points.

[159] Ethereum.org JAVASCRIPT API LIBRARIES https://ethereum.org/ja/developers/docs/apis/javascript/

[160] Ethereum.org NODES AND CLIENTS https://ethereum.org/ja/developers/docs/nodes-and-clients/

(4) 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.

(5) Generic codes used in 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.

(6) 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.
- The Wallet terminals, operational servers, infrastructure providers, and Ethereum nodes in Figure 2-7-1 are dependent on the Internet, and the Internet is considered to be a trust point.

(7) 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.
- The Oracle in Figure 2-5 is dependent on the external Oracle, and the external Oracle is considered to be the trust point.

(8) 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.
- The Maker protocol in Figure 2-3-1-1 relies on an external BOT, the auction keeper/market maker keeper, and the auction keeper/market maker keeper is considered to be a trust point.

(9) 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.
- The voter in Figure 2-7-2 depends on the code content of the proposer's smart contract, and the proposer is considered to be the trust point.

(10) 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 holder to whom they have delegated their vote vote as they expect.
- Individual investors in Figure 2-3-3 Maker rely on voting proxies, and voting proxies are considered to be trust points.

(11) 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 correctly and promptly deploys what has been passed.
- The proposer in Figure 2-7-2 is dependent on the deployment work of the administrator or authority, and this administrator or authority is considered to be a trust point.

(12) 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 correctly modify the smart contract and respond without causing any damage.
- Investors and users in Figure 2-5 rely on the DeFi System Development Tool via the DeFi Protocol Interface, and the DeFi System Development Tool is considered to be a trust point.

(13) 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.
- The voters (including users) in Figure 2-7-2 are dependent on the legitimate actions of the proposal cancellation authority, and the proposal cancellation authority is considered to be a trust point.

(14) 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)
- The Ethereum blockchain and Sidechain in Figure 2-5 rely on a two-way bridge fund lock, and the two-way bridge is considered to be a trust point.

2-7-2 Analysis of Weakest Link

(1) 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)
- Of the multiple layers of other blockchains in Figure 2-5, the Weakest Link would be the validator's private key management in the Sidechain of the blockchain layer.

(2) 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 (Exsample: Beanstalk Incident).

- Of the components that make up governance voting, such as DeFi protocols, voting rules, proposers, and voters, the Weakest Link would be the rule deficiencies in governance voting, where the role of verifying proposals was not made clear to anyone.

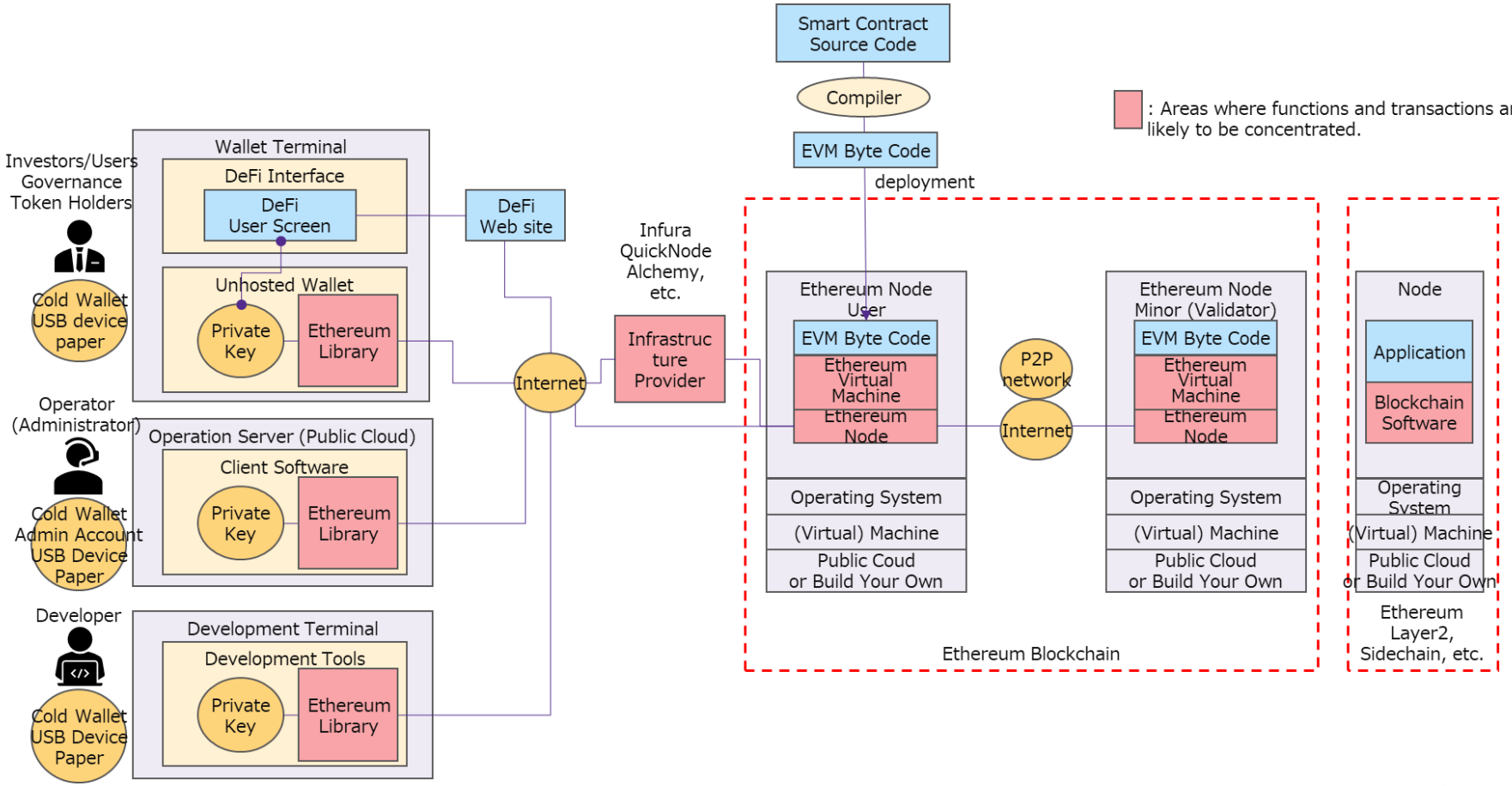


Figure 2-7-1 Analysis of trust points in the chains of trust (wallet terminals, operational servers, and Ethereum nodes)[161]

[161] Ethereum.org NODES AND CLIENTS https://ethereum.org/en/developers/docs/nodes-and-clients/

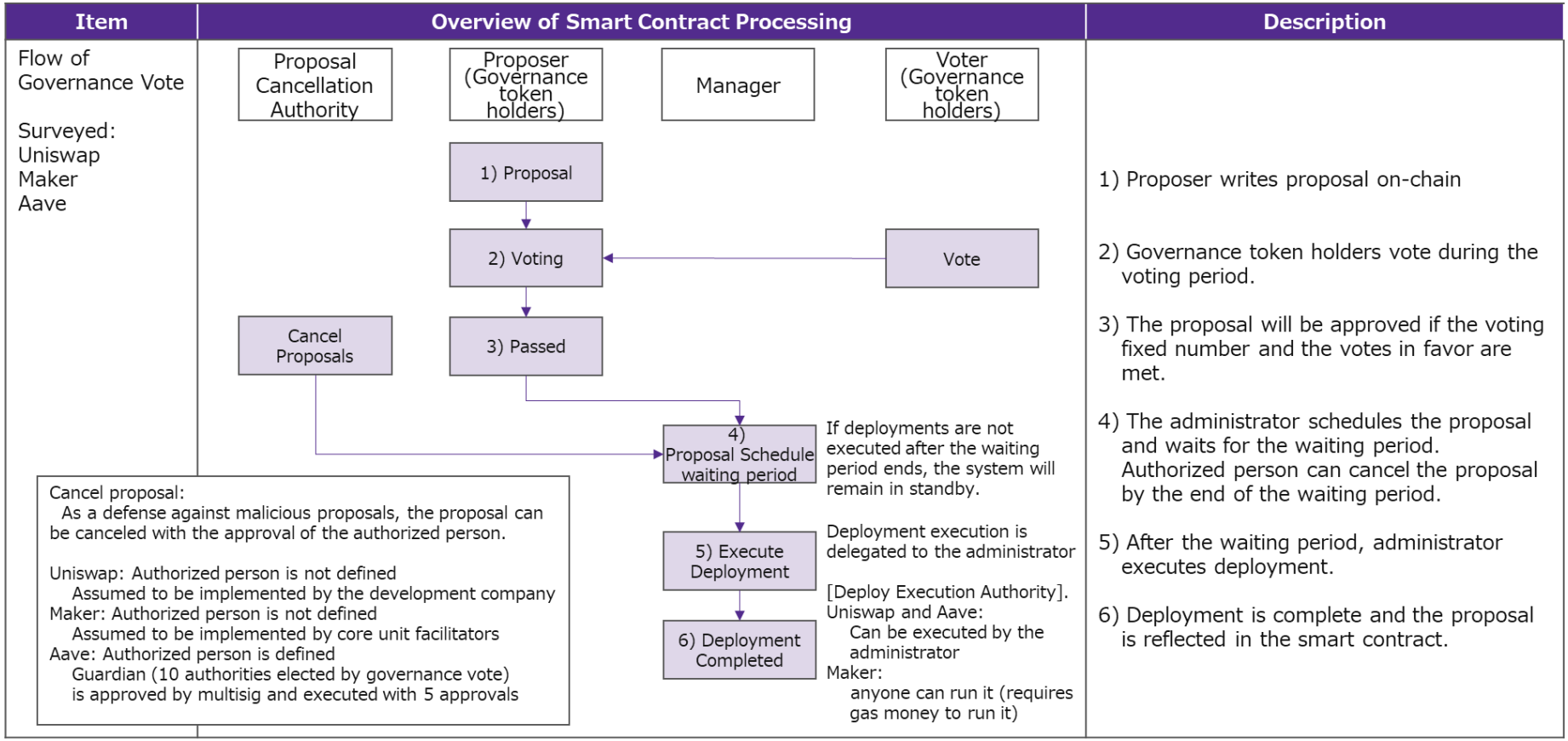


Figure 2-7-2 Analysis of Trust Points in the Chains of trust (Governance Voting and Deployment)[162]

[162] Uniswap Governance Smartcontract https://github.com/Uniswap/governance/tree/master/contracts
Maker Governance Smartcontract https://github.com/makerdao/governance-portal-v2
Aave Governance Smartcontract https://github.com/aave/governance-v2

Chapter 3. Identifying Risks in a Decentralized Financial System

In this chapter, we attempted to identify the major risk factors in decentralized finance based on the major components of a decentralized financial system identified in Chapter 1 and the results of the analysis of major DeFi projects and incident cases in Chapter 2. In this chapter we summarized each risk event and discussed the possible risk factors in the view points of System Operation in 3-1, System Development in 3-2,Governance in 3-3, and 3-4: Engagement with Financial Markets in 3-4.

In addition, among the items listed below, there are issues that are particularly closely related to DeFi (i.e., those that are exclusively necessary for DeFi functions, services, and operations) and those that affect not only DeFi but also crypto-assets and blockchain in general. While emphasizing that this distinction has nothing to do with the importance of ensuring security, etc., and that the line between the two is not always clear, Chapter 4 discusses risk mitigation measures, focusing on issues that are particularly close to DeFi.

3-1 Identifying Risk Factors in System Operation

(1) Hardware

Table 3-1-1 Risk Factors in System Operation (Hardware)

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
PC/Smartphone	-	- PC/smartphone malfunctions and the wallet is temporarily unavailable.	- No spare PC/smartphone (a spare unit can be substituted)	X General Equipment Failure
Server Equipment	-	- Transaction cannot be executed due to equipment failure of Ethereum node.	- No spare node is prepared.	X General Equipment Failure
Public Cloud	Failure of bases and simultaneous shutdown of many servers	- A power failure or other malfunction at a location in the public cloud causes many nodes to stop simultaneously, preventing the execution of many transactions. - Due to a problem in applying OS patches to servers in the public cloud, many servers became unavailable at the same time, and transactions could not be executed.	- Public cloud contracted at a single location	X Public Cloud Usage Issues
Cold Wallet	Loss or unavailability of cold wallet private key	- The cold wallet device (e.g., USB flash drive) fails and the user's	- Not prepared to back up cold wallet equipment (Metamask	X General Equipment Failure

		private key is not available, rendering the wallet unusable.	recommends paper)	
		- The user's private key or mnemonic sequence printed and stored in a cold wallet is lost, and the wallet becomes unusable.	- The paper on which the user's private key or mnemonic sequence is printed is not properly stored (forgotten where it is stored, accidentally destroyed, etc.).	X Private Key Management Issues
	Theft of Cold Wallet Private Keys	- The user's private key or mnemonic sequence is printed and stored as a cold wallet on a piece of paper, and the attacker uses the user's private key to steal the funds.	- The paper on which the user's private key or mnemonic sequence is printed is not kept as an important item (e.g., not kept locked).	X Private Key Management Issues
		- The private key is stolen by unknowingly using a cold wallet with malware, etc. installed.	- Difficult to tell from the outside that it is a secure cold wallet	X The problem of how to identify secure cold wallets

(2) Fundamental software network

Table 3-1-2 Risk Factors in System Operation (Infrastructure Software and Network)

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
Operating System	Malware	- Wallet terminals and operation servers are infected with malware through targeted attacks, etc., resulting in theft of users' private keys and unauthorized locking of data (ransomware attack).	- No measures to protect against malware (e.g., applying the latest patches, obtaining backups, education on the latest malware countermeasures, etc.)	X General Anti-Malware Issues
	Operating System Vulnerabilities	- Vulnerabilities in the node's OS (Linux, Windows, etc.) are discovered and	- Failure to implement a mechanism to promptly apply	X General Operating System Issues

		exploited before they are fixed (internal data leakage, tampering, etc.).	OS fixes and patches	
Internet	Communication failure, data leakage	- Internet communication failures (problems with communication infrastructure such as providers and carriers) at wallet terminals, operational servers, Ethereum Node, etc., may result in the inability to use funds or other operations, leakage of communication data, or other risks.	- When P2P network nodes of the same nature are structured in such a way that they do not trust each other, the joint points between P2P networks of different quality can be vulnerable unless they rely on some external references or join those P2P networks on the same node. The joint point can be vulnerable - Possible risk of data leakage, depending on the method of connection to the infrastructure provider	X Issues related to how P2P networks and infrastructure providers connect via the Internet

(3) Blockchain infrastructure

Table 3-1-3 Risk factors in system operation (Blockchain infrastructure)

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
Blockchain	Processing delays due to chronic increase in transactions	- There is concern that the increased volume of DeFi transactions running on Ethereum will cause chronic congestion on Ethereum, resulting in processing delays and transaction failures. - Ethereum congestion is not inherently solved by using 2nd	- Scaling measures for the Ethereum main chain have not yet been implemented. - However, Ethereum 2.0 sharding is currently in transition and will be completed in 2023.	X General Blockchain Issues

		Layer, a scaling solution, or other blockchains.		
	Ethereum Gas price soars	- Gas prices soar as Ethereum transactions increase. - There is concern that a high spike in gas prices will cause small users to leave Ethereum and the DeFi project to run out of liquidity funds.	- Gas prices are rising because Ethereum scaling measures have not yet been implemented. - However, layer 2 solutions, side chains, tiered chains, and other low gas cost environments are already available.	X General Blockchain Issues
	Rapid increase in transactions due to market impact	- The network becomes congested due to large transaction volume caused by external factors such as a market price collapse, which leads to high gas prices and transaction delays.	- When the market price of a crypto-asset crashes due to unforeseen external factors, the entire price of the crypto-asset fluctuates due to a chain of trades. - Further increase in transactions in response to the market	X Blockchain Network Issues
	Dependence on P2PNetWork	- Users trust that the P2PNetwork will not be shut down, and do not assume that a malfunction will cause the network to be shut down.	- Users are not considering how to respond in case the P2PNetwork goes down.	X Blockchain Network Issues
	Front Running Attack, Sandwich Attack	- Miners and validators intentionally insert their own transactions before or after the transaction to preempt the market price and earn a profit margin. - Miners and validators deliberately rearrange the order in which transactions are processed to	- There are strategic minors and validators (acting in one's own favor). - Due to the way the blockchain works, strategic miners and validators cannot be eliminated.	X Blockchain Mining and Validation Issues

		increase the cost of gas.		
	Mining Monopoly	- 51% attack (monopolizing more than 50% of the entire network's mining rate) allows malicious miners to dominate the mining, making it impossible to guarantee legitimate operations, such as validating falsified transactions.	- Malicious minorities exist. - The blockchain mechanism does not eliminate malicious miners.	X Blockchain Mining Issues
	Decreased Incentives for Minors	- If the incentive for miners is reduced in a proof-of-work market environment (miner compensation < mining costs), miners will be reluctant to perform mining, and legitimate operations cannot be guaranteed.	- Miners will not mine without reward incentives.	X Blockchain Mining Issues
	Validator Collusion	- When Proof of Stake validators collude (validators are fixed and free market competition is eliminated), malicious validators dominate the validation and cannot guarantee legitimate operation.	- Malicious validators exist. - The blockchain mechanism does not exclude malicious validators.	X Blockchain Validation Issues
	Hard fork of the Platform	- A hard fork of the entire platform to recover from the damage caused by a single application attack (Exsample: The DAO attack).	- Platform specification changes due to platform hard fork (DeFi protocol may need to be supported, but whether or not users need to	O Blockchain update could have major impact on DeFi protocol

			respond depends on the situation.) - Hard forks of the platform are ultimately decided by the platform administrators (e.g. Ethereum Foundation).	
	Dependence on Blockchain	- Users trust that the blockchain will not fork (branching of the blockchain due to updates such as specification changes). - For example, the company does not anticipate that a hard fork will cause a drop in the price of the tokens or a suspension of some transactions.	- Users are not considering how to respond in case the blockchain forks.	O Blockchain update could have major impact on DeFi users
	User Privacy Protection	- All blockchain transactions are public, so transactions and balances at users' addresses become public (transaction history can be seen by others, addresses with a large number of tokens held are more likely to be targeted by attacks, etc.) - However, the address is not linked to the individual user.	- Concerns that the emphasis on transparency and security through public disclosure of transactions has led to a lack of emphasis on privacy protection.	X Blockchain Specification Issues
Software Wallet (Hot Wallet)	Attacks on hot wallets	- Wallets that hold large amounts of tokens, such as large governance token holders and community fund managers, are vulnerable to attackers.	- Large holders of tokens exist (large numbers of tokens are held at a particular address). - Wallet address and token count	O Concentration of funds to specific addresses in DeFi

			are publicly available	
	Service shutdown at wallet vendor	- Hosted wallet services cease due to bankruptcy of wallet vendor, etc., and wallet funds become unavailable.	- Hosted wallets stored by wallet vendors will no longer be available - (Other wallet vendors may be available if they have the user's private key)	X Wallet Vendor Management Issues
	Undesirable Wallet Usage	- The user is not aware of the existence of undesirable wallets, such as those with security or quality problems, and uses them without being aware of it.	- Users are not willing to research secure wallets on their own (e.g., users with low literacy). - No information is disclosed on the safety of the wallet application, and there is no mechanism for disclosing information.	X The problem of how to identify secure wallets
Software (excluding OS)	Software Vulnerabilities (Wallet, client software, etc.)	- Software vulnerabilities can disrupt wallet and system client software, temporarily disabling wallet usage and system operations.	- Not prepared for service interruptions due to software vulnerabilities (e.g., use of multiple wallets and client software)	O Potential impact on DeFi users due to loss of access to wallets, etc.
	Vulnerability in Ethereum libraries (Web3.js, ethers.js, etc.)	- If a critical vulnerability is discovered in the Web3.js library or other libraries and this library becomes unusable, many services will be affected because Ethereum cannot be connected from the outside, such as wallets and system operations. - *Web3.js library and other libraries are common Ethereum blockchain access	- Not prepared for service interruptions due to library vulnerabilities (e.g., use of multiple wallets and client software) - Users are concentrated in certain libraries - Development structure of libraries may be person-oriented (e.g., ethers.js has one developer and maintainer).	O Library vulnerability may affect DeFi services

		software, and vulnerabilities can have a significant impact on external connections.		
	Ethereum Node Software Vulnerability	- Software vulnerability in Ethereum Node prevents communication between nodes, rendering the entire Ethereum inoperable. - Ethereum Node and Ethereum Virtual Machine are node-common software (development language and implementation differ for each node), and if a defect occurs, the corresponding node will become inoperable. - If any software contains a vulnerability, all nodes that use it are affected by the vulnerability.	- Nodes are not prepared for node shutdown due to software vulnerabilities (prepare nodes considering multiple languages and implementations) - Users are concentrated on specific implementations of the software.	O Ethereum node software vulnerability may affect DeFi services
	Dependency on Ethereum library and Ethereum Node software	- DeFi developers trust that the Web3.js library and Ethereum Node software are defect-free	- We have not considered countermeasures in the event of a problem with the library (e.g., changing to alternative software, use of multiple software, etc.).	O By design DeFi's system structure that requires the use of applicable software.
	Discontinuation of Ethereum library offerings by developers (e.g. Ethereum Foundation)	- There is a concern that wallets will not be able to securely connect to Ethereum if the Web3.js library or other libraries are discontinued due to the suspension	- It is not clear whether the library can be continued to be operated by other volunteers even if the developer does not operate the library (if the library cannot be continued to be	X General management issues of the library developer used by DeFi, but with a certain impact on DeFi

		of the developer's activities, etc.	used, the impact on users will be significant).	
	Lack of diversity in Ethereum library and Ethereum Node software	- Common software is initially diversified by various specifications and implementations, but as it is used, there is concern that it will converge on a single one and become more concentrated.	- There is no mechanism to maintain and manage the diversity of common software developed by common software developers (e.g. Ethereum Foundation) with multiple specifications and implementations.	O Multiple implementations of libraries and software used by DeFi are DeFi specific issues
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.	O Primarily DeFi users use infrastructure providers
	Interruption of services provided by infrastructure providers	- 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 are not considering how to respond to possible service outages of infrastructure providers (e.g., use of multiple providers).	O Primarily DeFi users use infrastructure providers
	Dependence on infrastructure provider services	- 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 respond in case of service outage by infrastructure providers.	O Primarily DeFi users use infrastructure providers

(4) Application infrastructure and applications

Table 3-1-4 Risk Factors in System Operation (Application Infrastructure and Applications)

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
DeFi Protocol	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 means of emergency - Blockchain specifications usually do not stop smart contracts, so the DeFi protocol must have measuresfor emergency.	O
	Emergency Procedures	- There is a concern that services may be affected due to the inability to respond quickly in the event of unforeseen events (market price collapse, external attacks, etc.). - The measures plan for unforeseen circumstances may not be clear.	- Not having contingency policies and procedures in place - Failure to implement contingency mechanisms and functions	O
	Identification of DeFi protocol users	- If the user is a pseudonym, the attacker/victim cannot be identified at the time of the incident.	- DeFi projects do not usually ask users for KYC	O
	Prevention of outflow of funds	- Many DeFi protocols do not have the ability to freeze funds in the event of an external attack, which increases damage.	- No contingency measures, such as a token freeze function, have been incorporated.	O
	Withdrawal of funds when DeFi protocol is stopped	- If a vulnerability or other defect in the DeFi protocol causes a service shurtdown, funds	- No countermeasures against withdrawing funds from liquidity	O

		cannot be withdrawn until the service is restored.	pools, collateral pools, etc. in the event of DeFi protocol outage	
	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.	- Flash Loan requires no collateral had no limit in loan amount (however, there is a disadvantage of high fees when borrowing large amounts of money, and advanced knowledge is required to earn a profit)	O
Oracle	Oracle Attack	- External attacks target vulnerabilities in Oracle pricing - (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 - Of the DeFi projects, Oracle prices may be linked to market prices for specific projects	O Oracle vulnerability is a DeFi specific problem
	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 the oracle price is intentionally delayed, the oracle price cannot keep up with sudden changes in market prices, resulting in a large difference.	O Reflecting oracle prices is a DeFi specific problem

3-2 Identifying Risk Factors in System Development

Table 3-2 Risk Factors in System Development

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
Software (excluding OS)	Risks of code running in a web browser	- If a vulnerability is discovered in code such as the Defi protocol interface executed	- DeFi users may enter their private keys and other information from the wallet screen	X Code that runs in web browsers is used by other software, etc.,

		by a web browser, there is a risk that the wallet's private key can be stolen.	provided in their web browser, and there is concern that they may be vulnerable if the vulnerability is discovered.	and is not an issue closely related to DeFi
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. - The problem is that the expected correction cannot be made when there is a problem related to upgradability.	- It is extremely difficult to eliminate all vulnerabilities in smart contracts, and non-upgradability is considered risky.	O Smart contract design is a DeFi specific problem
	Smart contracts upgradeable	- Enforcement of upgrades is based on the assumption that there are no vulnerabilities (generally software is assumed to be vulnerable, but smart contracts are not allowed to be vulnerable because vulnerabilities can lead directly to losses or attacks)	- Transactions executed on the blockchain cannot be undone (basically, it is not possible to rewind an already executed transaction or correct past amounts). - This leaves the smart contract vulnerability unacceptable, even if it is upgradable.	O Smart contract design is a DeFi specific problem
	Code Vulnerability	- Incidents using publicly known code vulnerabilities are recurring, and vulnerabilities are not preventable. i) Reentrancy vulnerabilities (The DAO, Uniswap, etc.) ii) Flash Loan attacks (bZx, Harvest Finance, etc.)	- Smart contracts have complex features and it is technically difficult to detect all vulnerabilities.	O Smart contract vulnerabilities are a DeFi specific problem

	Intrusion of malicious code	- Smart contracts are externally vulnerable due to malicious code embedded in generic code imported from the supply chain, etc.	- When using generic code, the program specification is not verified (or the skills to verify are not available).	X Malicious code is a common problem with software
	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.	- Testnet cannot confirm transactions related to incentives, so they may be deployed on the main net without adequate testing (Testnet: same functionality as the main net, but no transaction fees, different transaction congestion, etc.)	O The Testnet environment is a DeFi specific issue
	Smart contract malfunction	- Even if funds are lost due to a malfunction of a self-created smart contract (e.g., a discrepancy in the remittance address), the funds cannot be recovered because they cannot be corrected.	- Testing and code auditing cannot verify all smart contract behavior	X Smart contract malfunction is a DeFi specific technology issue, but it is a user's own problem and has limited impact
	Secure advanced development engineers	- It is difficult to secure highly skilled engineers who can develop vulnerability-free code for complex processes such as reentrancy (reentrancy vulnerability occurred in The DAO and reoccurred in Uniswap 4 years later).	- Security technology required for the development of smart contracts has not been established. - There are no indicators to measure the technical skills of smart contract development engineers.	X Problem of securing development engineers
	Skills Issues for Development Engineers	- Inexperienced engineers developing the program may	- If engineers do not know the existing development	X General System Development Issues

		cause quality degradation and degrade	rules and quality control methods, they cannot ensure a certain level of quality.	
	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).	- Smart contract attacks are becoming more sophisticated, and the specialized skills of code auditors and the validation techniques of auditing tools are not keeping up with new or complex attack patterns.	O Code audit is a DeFi specific issue
Blockchain	Attack on funds locked in two-way bridge	- Heavy losses due to validator private key theft attacks targeting funds locked in two-way bridges between Ethereum and sidechains (Example: March 2022 Ronin Network). - 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.	- Ethereum specifications lock large sums of money in two-way bridges for exchange of funds with sidechains, making them vulnerable to attackers.	O Exchange of funds between blockchains is a DeFi specific problem
	Connections between blockchains	- External attacks targeting vulnerabilities in processing across the blockchain. - Cross-chain smart contract invocation vulnerability case study (PolyNetwork) - Example of signature verification	- The complexity of transactions across the blockchain makes it difficult to verify with testing (test cases are not comprehensive, lack of anomaly testing, boundary condition testing, etc.)	O Interlocking smart contracts between blockchains is a DeFi specific problem

		vulnerability in the Token Bridge Protocol (Wormhole)		
	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. - 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. - No mechanism to compare and disclose information on vulnerabilities of platforms	O Interlocking smart contracts between blockchains is a DeFi specific problem
DeFi Protocol	Defects in some functions of DeFi protocol (leakage of consideration during gas price increase)	- 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).	- The business process for the DeFi project does not take into account the ability to keep up with the gas price of one's transaction in the event of a sudden gas price spike.	O
	Defect in some functions of DeFi protocol (leakage of prevention of zero bidding)	- Zero-bid processing drains funds while the original process is stuck due to soaring gas prices.	- No built-in process to prevent transactions that are not supposed to occur, such as zero bidding.	O
	Interlocking between DeFi protocols	- Interlocking between DeFi protocols can be exploited to break assumptions made by external factors (e.g., Oracle pricing) - Huge sums of money borrowed	- No maximum transaction amount (e.g., liquidity pool deposit amount) - The design does not take into account the fact that the system can be linked	O

		through Flash Loan (unsecured and unlimited) are put into liquidity pools of other DeFi protocols, causing a sudden change in the price of Oracles - 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.	from various DeFi protocols.	

3-3 Identifying Risk Factors in Governance

Table 3-3 Risk Factors in Governance

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
Governance Voting	Governance Voting Control	- Voting is dominated by a small number of major governance token holders with enough votes to constitute a quorum for passage - Voting is controlled by the community and developers, who hold large amounts of governance tokens, including those for system use.	- Governance tokens are bought and sold on the crypto-asset market, which is structured so that those with the money get more votes (DAO decision-making is not decentralized) - Unlimited number of governor tokens	O
	Governance Voter Pseudonyms	- Governance voting is conducted under pseudonyms, which may make it impossible to identify the party to be held accountable for	- There is no mechanism to link user account addresses to individuals.	X It's a problem with how the blockchain works, not DeFi specific.

		the outcome of the vote.		
	Quorum to vote is not high	- 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 Governance Vote likely means fewer quorums to pass proposals	O
	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 - Governance token holders are not motivated to vote (there is no mechanism to motivate them)	O
	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 It is not clear whether verification of malicious proposals will be ensured.	O
	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; the majority are for-profit - Insufficient disclosure of information on smart contract	O

			modifications, and no assurance of the validity of comments presented in community forums, etc.	
	Organization of DAOs	- DAOs have unclear representatives and boards of directors, making it difficult to hold them accountable when problems occur. - DAO has no organization to pursue.	- The DAO is an organization of non-trusting participating members and has no representatives. - There are no laws and regulations applicable to DAOs, and the shape of the organization is not yet defined.	O
	Location and membership of DAO	- The location of the DAO is unclear. - DAO members are dispersed throughout the world and cannot be regulated or pursued across national borders.	- The DAO is not registered with any public agency and its location is unclear. - It is unclear which country's laws and regulations apply.	O
DeFi Protocol	Lack of awareness of DeFi Protocol Terms of Use	- There is a concern that users may use the service without knowing the contents of the DeFi Protocol Terms of Service and incur losses.	- DeFi protocol terms of use (user's own responsibility) are not made available to users before using the service.	O

3-4 Identifying Risk Factors in Engagement with Financial Markets

Table 3-4 Risk Factors in Engagement with Financial Markets

Main items	Sub items	Risk events	Possible risk factors	Issues closely related to DeFi
Crypto-asset Market	Lack of backstop functionality in the crypto-asset market	- In the event of a systemic risk such as a price collapse of fiat currency in the financial market, the central bank of each country functions as a backstop, but	- No mechanism to stabilize the price of tokens when they fall in the crypto-asset market	X Issues related to the crypto-asset market in general

		there is no backstop function in the crypto-asset market. - When systemic risk materializes in the crypto-asset market, the market as a whole is greatly affected. - The company has actually experienced major crashes such as Black Thursday in March 2020, and it was difficult to take countermeasures.		
	Insufficient explanation of risk of loss	- There is a concern that ordinary investors with little expertise may trade without knowing the risks of volatile crypto-assets and suffer losses.	- No mechanism to make users aware of the risk of loss in transactions.	X Issues related to the crypto-asset market in general
DeFi Protocol	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	O Issues with DeFi applications and connected financial institutions
	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.	- Risk of loss associated with the use of DeFi protocols, which may have latent vulnerabilities, and with holding volatile crypto-assets	O Volatility issues with crypto-assets used in the DeFi protocol
	Insufficient explanation to users	- There is a concern that users may be unaware of the differences between DeFi Protocol's terms	- The system is not designed to warn users of the differences from fiat currencies and what to do in case of damage	O Accountability issues for DeFi users

		and conditions and disclaimers from those of general financial services, or that DeFi Protocol's response in the event of loss (no compensation for loss) may result in a loss.	before transactions are made.	
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).	O Smart contract functionality is a DeFi specific issue

Chapter 4. Analysis of Risk Mitigation Measures in a Decentralized Financial System

This chapter attempts to discuss specific risk reduction measures and proposed countermeasure plans in supervision by authorities for DeFi-specific issues among the risk factors identified in the previous chapter.

In 4-1, we analyze risk mitigation measures and proposals for their implementation from the perspective of system operation, in 4-2, system development, in 4-3, governance, and in 4-4, engagement with financial markets.

With regard to the risk mitigation measures analyzed, as noted above, there are multiple areas where trust points in a decentralized financial system are concentrated, which means that they have the same risks as existing financial institutions, and risk mitigation measures are expected to be as centralized as those of existing financial institutions.
However, as decentralized financial systems become more diversified, the risk reduction measures analyzed in this report may not always be available, and therefore, we believe that the content of the measures needs to be reviewed.

There is also a need to ensure that trust points are correctly identified by DeFi project management organizations and users. Regarding the multiple trust points detected in the analysis of this study, there is no particular discussion about trust points in the DeFi project community, etc., and there is concern that the DeFi project management organization and users do not correctly recognize trust points. Therefore, it is important to make the trust points correctly recognized by the DeFi project management organization and users.

Since the discussion is premised on the assumption that the DeFi project and blockchain management organizations are cooperative in the implementation of risk reduction measures, it is necessary to consider a mechanism to obtain cooperation in the implementation of the measures.

4-1 Analysis of Risk Mitigation Measures in System Operation

Table 4-1-1 Risk mitigation measures in system operation

Main items	Sub items	Possible risk factors	Risk reduction measures (Proposal)	Notes, etc.
Software (excluding OS)	Ethereum library and Ethereum Node software diversity is compromised.	- Common software may be equipped with multiple specifications and implementations, but over time they converge into a single one, and there is no mechanism to maintain and manage diversity.	- The developer's organization (e.g. Ethereum Foundation) recognizes the risk of this issue and implements a mechanism to distribute users across multiple software. - For organizations that are subject to the oversight of the authorities, make it a condition that design diversity is met in the procurement of software (i.e.,	- There is a concern that blockchain management organizations are often global organizations, making it difficult to coordinate from Japan. - Even if distributed among multiple software, continuous monitoring, including usage, is necessary to prevent convergence to a single software due to

			make the preparation of multiple pieces of software with differing specifications and implementations a condition). - Devise conditions of use so that there are no differences in convenience between software, and avoid concentration of use. - If software dispersion is difficult, use software development quality improvement measures to solve the problem.	convenience or other reasons.
	Dependency on Ethereum library and Ethereum Node software	- Dependence on the quality of the software and its continued availability to users, and lack of consideration of what to do in the event of non-availability.	- The developer's organization shouldl inform users of the risks of the case.	- Need to consider ways to reach out to developer organizations
	Hot Wallet Attacks	- Large token holders are vulnerable to attack because their account addresses and token holdings are publicly available (if they hold a large number of tokens at a particular user account address).	- Blockchain specifications make it difficult to keep account addresses and token holdings of large token holders private. - As a countermeasure, disseminate technical information to large token holders on how to securely store	- Regulatory authorities or equivalent bodies need to consider rules to verify and certify highly secure user private key storage technologies and make them known to users. - Examples of private key storage technologies

			users' private keys.	i) Secret sharing: Private keys are divided into multiple keys and stored separately by multiple people (use case confirmed at expert interviews). ii) Social Wallet: A social wallet is a wallet in which a trusted friend or acquaintance is entrusted with the custody andright to change the public key. - Trusted acquaintances/ friends with the right to change the public key and entrust the custody of the key to them. - Since there are multiple wallet technologies, it is important to provide users with options (from expert interviews)
Infrastructure Provider	Concentration of use of services provided by 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). - Recommend using multiple infrastructure providers depending on the severity of	It is necessary to make users with low literacy aware of the risks involved.
	Dependence on infrastructure	- Users rely on infrastructure providers to		

	provider services	keep their services up and running.	the DeFi service shutdown	
	Suspension of services of infrastructure providers	- 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 - Infrastructure providers obtain quality certification (SOC2) to reduce the risk of service shutdown	- Possible measures to be taken include i) Chaos Engineering: A method of injecting failures into the production environment and keeping recovery functions running at all times, as implemented by Netflix and AWS. ii) SOC2: (System and Organization Controls 2) Use the internal control and assurance reporting framework at the outsourcing provider (trustee company)
DeFi Protocol	Unlimited borrowing of funds through Flash Loan	- Users can borrow crypto-assets with no collateral and limist. (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. i)Set collateral amount when using Flash Loan (n% of borrowed funds) 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	- No consideration of emergency shutdown of DeFi protocol as a measure of emergency	- Instruct the DeFi project to create a feature that allows for emergency shutdown of the DeFi protocol in	- We believe that it is extremely difficult to develop a complete smart contract that is

		- Smart contracts cannot be stopped by blockchain specifications, so the DeFi protocol must be used.	the event of an emergency.	unaffected by an attack. - Therefore, it is important to have an emergency shudwown function as a measure of minimizing damage in the event of an emergency.
	Measures for unforeseen circumstances	- Not having contingency policies and procedures in place - Failure to implement contingency mechanisms and functions	- DeFi projects develop contingency plans for unforeseen events and identify necessary system measures. - Implement responses the mesures such as external Oracle suspension, DeFi protocol emergency shutdows, etc., in accordance with that policy. - 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. - Maker has established five major contingencies and has developed contingency plans for them. - Periodic training could include methods such as hardening. *Hardening: To split a team into two teams of operators and attackers to actually attack and defend to gain hands-on experience.
	Prevention of outflow of funds	- DeFi protocols may not consider contingency plans, such as the loss of funds due to an attack	- Because the DeFi protocol is at high risk of attack, blockchain governing bodies should guide the rulemaking and implementation of measures to	

			prevent the loss of funds in the event of an attack.	
	Withdrawal of funds when DeFi protocol is stopped	- No means of withdrawing funds from liquidity pools, collateral pools, etc. in the event of DeFi protocol shutdown	- Instruct DeFi projects to establish the ability to withdraw a certain amount of funds in an emergency (but there is concern about the risk of attack).	- The inability to withdraw funds is a serious risk for user protection and must be addressed. - To reduce the impact in the event of an outbreak, measures such as limiting the amount spent by making users aware of the risk could be considered.
Oracle	Oracle attack	- Oracle pricing methods vary from DeFi project to project, and no safe implementation method has been established - 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 imforming users of safe Oracle usage.
	Delay in reflecting external 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.		

Based on the analysis of risk mitigation measures for system operations, the following risk mitigation measures are noted as particularly important

a. Lobbying blockchain governing bodies (e.g. Ethereum Foundation)

There is concern that the concentration of the use of Ethereum libraries and common software will prevent the elimination of SPoF, which is a benefit of a decentralized financial system, and is

an issue that has the same centralized risk as existing financial institutions. We believe that it is important to continuously monitor this issue to avoid convergence to a single one by intentionally preparing multiple libraries and softwares, etc., and that feasibility should be examined.

b. Ensure that users are aware of the safe usage of Wallet DeFi

We believe that it is necessary to protect users from being disadvantaged by introducing a mechanism to identify and inform users of how to use wallets and DeFi safely, so that they can have high literacy about these topics (e.g., authentication by a certification authority, issuance of a guiance, or notification of risks).

4-2 Analysis of Risk Mitigation Measures in System Development

Table 4-2 Risk Mitigation Measures in System Development

Main items	Sub items	Possible risk factors	Risk reduction measures (Proposal)	Notes, etc.
Smart Contract	Smart contract not upgradeable	- 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., OpenZeppelin Upgrades Plugins), so it is important to consider which service to deploy.
	Smart contracts upgradeable	- The specifications of the blockchain make smart contracts vulnerable because transactions that have been executed cannot be undone later (basically, it is not possible to rewind an executed transaction or correct past amounts, etc.).	- DeFi protocols could reduce risk through reverse transactions that cancel past transactions (e.g., reversing a money transfer transaction to return funds) - We believe that the feasibility and effectiveness of reverse transactions require further study.	- Blockchain specifications do not allow for the reversal of past transactions, but there is a possibility that past transactions can be reversed through an automatic reverse transaction mechanism.
	Code Vulnerability	- Developers and code auditing companies have technical difficulty detecting all vulnerabilities from the	- In developing the DeFi protocol, use the latest technology to ensure the quality of software	- Need to consider ways to reach out to blockchain management organizations

		complex functionality of smart contracts.	development and eliminate vulnerabilities as much as possible. i) Formal verification ii) Automated testing by machine learning, etc. - The blockchain governing body should be responsible for sharing case studies and recommending technologies to be developed.	
	Test verification constraints	- 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. - 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	- 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. - Code auditing firms should collaborate on a system for technical improvement (e.g., by holding periodic competitions	- Examples of analysis techniques for code auditing tools i) Static verification Verify smart contract code ii) Dynamic verification Verification while executing smart contracts iii) Formal verification - Using formal and mathematical methods, prove that the code is

			and ranking them).	correct in the light of the formal specification description and properties
Blockchain	Attack on funds locked in two-way bridge	- 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.) - 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 i) Secret decentralization ii) Social Wallet iii) Social Wallet - Review of specifications for two-way bridges requires feasibility study
	Connections between blockchains	- 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.).	(Same as 4-2 code vulnerability)	(Same as 4-2 code vulnerability)
	Main chain impact from quality issues with other blockchains and layer 2 solutions	- There are a number of blockchain and layer 2 solutions, some of which have vulnerabilities and other concerns. - 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.
DeFi Protocol	Defects in some	- Developers are not taking into	- Apply Ethereum and 2nd Layer	- The following scaling

	functions of DeFi protocol (Lack of consideration when gas prices soar)	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	scaling technology to create a mechanism that does not cause sudden gas price spikes	measures are planned and implemented - Use of Ethereum 2.0 (sharding, planned) - Use of 2nd Layer Solutions - Use of Side Chains
	Defects in some functions of DeFi protocol (Lack of zero bidding prevention leakage)	- 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. - 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.
	Interlocking between DeFi protocols	- DeFi protocol does not set a cap on the amount of transactions (e.g., the amount deposited in the liquidity pool) - 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 - Test validation methods should be included in the code vulnerability measures.	(Same as 4-2 code vulnerability)

Based on the analysis of risk reduction measures for system development, the following are considered to be the main risk reduction measures

a. Need to consider a mechanism to cancel past transactions

The specifications of the blockchain do not allow transactions once executed to be undone later, making smart contracts vulnerable to unacceptable conditions (basically, it is not possible to rewind an executed transaction or correct past amounts).

As a countermeasure, a mechanism that allows secure unwinding upon discovery of vulnerabilities (e.g., reversing a money transfer transaction to return funds) should be studied in the future, including feasibility and effectiveness.

b. Advanced Smart Contract Vulnerability Countermeasures

From the incident case studies, it is extremely difficult to completely eliminate vulnerabilities, as smart contract vulnerabilities have not been eliminated to this day, and incidents such as

reentrancy vulnerabilities that occurred in the past have recurred since then. From the information obtained from the expert interviews, the most advanced technologies have prepared advanced development tools such as automated testing by machine learning, which has increased the ability to detect vulnerabilities. However, the vulnerability of smart contracts is still far from being completely eliminated.

While the immediate countermeasure is to reduce vulnerabilities by having experienced developers, we believe it is important to continue to advance detection techniques to eliminate smart contract vulnerabilities in the future.

c. Preventing theft of funds locked in a two-way bridge

Up to billions of dollars of funds are locked in side-chain two-way bridges, which are targeted by attackers. As measures to reduce this risk, it is important to improve the sophistication of private key management technology and disseminate secure private key management methods. In addition, specifications for locking funds in two-way bridges should be considered so that large sums of money are not concentrated in one place.

4-3 Analysis of Risk Mitigation Measures in Governance

Table 4-3 Risk Mitigation Measures in Governance

Main items	Sub items	Possible risk factors	Risk reduction measures (Proposal)	Notes, etc.
Governance Voting	Not enough for a quorum to vote.	- 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. - Guidance to the governing body should be provided by the blockchain governing body
	Low voter turnout	- 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	
	Verification of malicious proposals	- In decentralized organizations, communities are free to participate and roles are not specified. - 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. - Set appropriate working periods (proposal time locks) to validate	- Guidance to establish rules for the governing body regarding the role of the verifier of the proposal and disclosure of its contents. - Guidance to the governing body should be provided by the blockchain governing body

			malicious proposals.	
	Dependency on smart contract modifications	- Only a small percentage of governance voting participants are technically capable of interpreting smart contracts - 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).	

4-4 Analysis of Risk Mitigation Measures in Engagement with financial markets

Table 4-4 Risk Mitigation Measures in Engagement with Financial Markets

Main items	Sub items	Possible risk factors	Risk reduction measures (Proposal)	Notes, etc.
Relationship with Financial Institutions	Risk of loss to financial institutions	- 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. - 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 loss to corporation			
Smart Contract	Market Stability	- 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 - Ability to reflect Oracle prices moderately in sudden price changes - The function to suppress the reflection of Oracle prices when price fluctuations

				exceed the base amount, etc.

Conclusion

This report describes the results of our research study on technological risks and other issues in chains of trust of the decentralized financial system. However, the decentralized financial system including DeFi is still in its infancy and continues to grow, with many NFT services and aggregators emerging, which are outside the central scope of this research study. In addition, since this research study was mainly concerned with technical risks of DeFi projects inside the blockchain, we are aware that we have not been able to comprehensively identify detailed risks for the external components of the blockchain. Therefore, the following items are pointed out as the main issues to be addressed in the future and investigated in depth in future activities.

Matters that need to be addressed in depth as issues for the future inculde

- Identify technological risks of the components that make up the wallet terminals and operational servers outside the blockchain.
  - Identify technogical risks covering operating systems, web browsers, wallets, client software, user interfaces, etc.

- Status Update on smart contract vulnerability detection technology
  - Technology for detecting smart contract vulnerabilities is still far from maturity, and although development tools using machine learning and auditing tools based on incident cases have been developed, it is necessary to continuously monitor the status of updates.

In addition, the risk reduction measures pointed out in this report are only examples, and in order to find the optimal risk reduction measures, it is essential to discuss the issues with stakeholders such as DeFi developers, business stakeholders, academia, and authorities to find solutions to the issues. For example, on the DeFi project side, efforts should be made to reduce vulnerabilities to ensure the quality of software development, and case dissemination and recommendations for development technologies should be made by the governing body (such as Ethereum Foundation) for the blockchain. On the part of the financial supervisory authority, it is conceivable that they will develop a framework for both innovation and necessary risk reduction, such as by securing engineers, etc. with knowledge of DeFi specifications and information security (code development, testing and verification techniques, etc.). We hope that this report will help to promote constructive dialogue among stakeholders in the future.