Whitepaper 2.0

Hyungsuk Kang

Nov 2022

Abstract

As a result of exploring the process of Terra and exchanges collapsing from 2022 and helping the SEC and the prosecution as witnesses in the investigation, the cryptocurrency ecosystem as we know it today has devolved into turmoil, with people ignoring and seizing the sovereignty of individual assets while claiming ambiguous decentralization that cannot be defined. Under the premise that decentralized money is created on top of a decentralized economy, Standard Protocol releases a white paper on version 2 of the protocol that protects individual digital assets and creates a more secure and sustainable decentralized economy.

Introduction

Standard may believe it has won the battle to develop better blockchain technology, but it has lost the battle to bring it to the masses. Standard was created to combat Terra, believing that it was unsustainable from the start and that it violated people's digital assets and privacy. Since then, we've made three technological breakthroughs in the last year.

First, EIP5252, a smart contract pattern standard that provides a safety device to protect individual assets when creating a decentralized economy, was registered as a draft. Second, we developed all the technologies related to the roadmap except for the completed version of the Oracle runtime module presented in the roadmap. Third, unlike MakerDAO, which stores **CDP** data in one contract as a linked list while creating an overcollateralized stablecoin, we were able to keep the gas cost constant and lower than MakerDAO while maintaining the same operation cost as aave by using the clone factory pattern.

Stablecoin technology is being developed, and in order to participate in the war to introduce stablecoins to other decentralized finance ecosystems, we examined the dynamics of existing decentralized finance and discovered that it was DeFi 2.0. However, the current DeFi 2.0 had a number of flaws.

DeFi 2.0 mainly competes with interest rates for tokens deposited by individuals, and is considered to be a form of entrusting funds to a specialized "algorithm" or "individual or group". Fei Protocol presented Protocol Owned Liquidity (POL)1 to collect asset liquidity in the name of providing liquidity to decentralized lending services with assets pooled together to earn more profits, and Olympus DAO2 raised the assets of individuals by issuing a bond that borrows existing Uniswap or Sushiswap **LP** tokens under the pretext of repaying the governance token of its decentralized autonomous organization at a very high-interest rate without collateral.
They all face problems, however, because they choose profit over economic independence and unconditional obedience over trust based on truth and verification. In the case of the Fei protocol, he borrowed money blindly to the Rari capital compound fork, and the hacking resulted in a massive loss3 of 80 million US dollars from assets collected from individuals. In the case of the Olympus DAO, there was no collateral for the value of its own governance token, and before the clear function of the governance token was announced, insiders began to sell excessively, resulting in a Ponzi scheme in which the last seller suffered the most damage. As a result, Standard prioritizes user deposit protection and openly discloses all funds deposited by users. We provide DeFi 3.0, which challenges the current decentralized financial system by allowing users to use their deposits more freely.

Standard 2.0

Standard 2.0 is implemented with the mission stated in the same abstract as 1. If there is a difference, tokenomics, decentralized exchanges, and stablecoins have been newly changed. Tokenomics turns into a membership token that grants sustainable demand and keeps the value of the token more stable. The decentralized exchange breaks away from the Uniswap fork in 1 and

launches Safe CEX, **New Order**. **USM** evolves from the pegging algorithm in 1 and turns it into a stablecoin called **SAFU**.

1. Justice

Currently, the tokenomics of cryptocurrency project tokens assert that "justice benefits the strong." When a cryptocurrency project receives investment, the governance and network tokens created are first allocated to venture capital and development team members. Team members can freely distribute those tokens. Even if governance is established, all agendas are decided by a single person with a large number of tokens. Is it then correct that justice was created to benefit the strong?

The sophistry that justice is beneficial to the strong reveals a contradiction in Plato's Book 1 of 'The Republic' as Thrasymachus and Socrates discuss the justice that constitutes the nation. Under the premise that an ideal state has justice, Thrasymachus says that 'what is beneficial to the strong' is the true justice of the world. For example, Thrasymachus argues that the rulers, interpreted as the strong, make laws and systems that are advantageous to them and tell the weak to follow them as justice, and through this, the world can only be led as the strong want. Therefore, the greed and corruption of the rulers, which are generally referred to as injustice, can be said to be true justice according to reason, and those who live contrary to it live an unhappy life of being used by the strong without realizing true justice. Upon hearing Thrasymachus' argument, Socrates refuted: “If it is right for the rulers to make decisions in their favor, then, on the other hand, can it be said that decisions in favor of the weak are wrong? But even rulers are human after all, so they can't always make the right decisions, right? If they make a mistake, it will be a decision that favors the weaker than themselves. Then the benefit for the strong you speak of is not justice, right?"

Trashymachus' rebuttal was straightforward: the ruler he was referring to was the ruler in the "strict sense." The "strict sense" did not refer to those who held the position of ruler, but to the concept of the ruler in general. The captain, for example, is the person who leads the crew and drives the ship to its destination. However, if a captain made a mistake and docked the ship in an unusual location, and if this is the captain's nature, then all captains should dock the ship in the incorrect location. However, a ruler in the 'strict sense,' that is, a captain who does his job 'well,' must dock the ship at the proper port, be recognized as the good strongman, and enjoy all the privileges mentioned before. In response, Socrates took doctors, captains, and horsemen as examples to figure out where the benefits of skills were headed. Socrates said, “A doctor's skill is beneficial to the patients they treat, a captain's skill is beneficial to the sailors he leads, and a horseman's skill is beneficial to the horses he keeps. Shouldn't the rulers you refer to, Thrasymachus, 'in the strict sense', then use their skills to benefit the weaker ones they rule?" Thrasymachus agrees with difficulty that every job or position

demands a price. However, rulers' remuneration or all gains obtained through greed and corruption, such as compensation received by rulers in the 'strict sense' only for ruling, are not of an inherent nature. This is because, in fact, a ruler is only a position and does not require specific skills. The profit-creating behavior of doctors, captains, and horsemen is only related to the so-called remuneration technique, and has nothing to do with the nature of rulers. And, rulers in the 'strict sense' must be the ones who rule the subordinates without any compensation.

Plato is said to have said, "The greatest cost of ignoring politics is being ruled by the bad people." In fact, it comes from the words that Socrates uses when criticizing those who do not care about the contradiction of the ruler in the 'strict sense' who has to rule the ruled any compensation. Socrates is concerned that the people are longing for a ruler of this "strict sense" as a politician. If you are a wise politician, you will not try to do politics as Socrates mentioned, and the greatest punishment they will receive is to be dominated by those who do not care about it and seek their own interests. This year, we watched helplessly as the rulers of the 'strict sense' that Trashmachos insisted on, and those of low quality, as Socrates put it, perpetrated deceptions and contradictions.

Do Hyeong Kwon claimed to be a messiah to save the existing world by creating decentralized money, and succeeded in having a frame of saving the cryptocurrency economy or the future monetary economy, but each time he avoided questions about the price or profit model or He was quick to criticize those who inquired about it. Do Hyung Kwon manipulated the total amount of Luna, and the foundation's wallet had 80 percent of the volume, which did not correspond to the distribution volume, but replaced it with an API and provided it to Coinmarketcap as information on market value measurement, and Coinmarketcap introduced the foundation as an exemplary case of providing API. In addition, the anchor protocol, which causes deficits due to violation of the loan-deposit margin, provides a stable profit of about 20% more per year than a bank that stores real money and uses the false fact to protect the money of people who work diligently and save money in the bank. Also, when comparing Anchor Protocol, which loses money due to a violation of the loan-deposit margin, compared to a bank that stores real money, they took the money of people who worked diligently and saved in the bank by putting forward the false fact that they would provide more stable profits of about 20% per year. Genesis Trading swapped `$10 million` worth of Bitcoin with UST to Terraform Labs without any disclosure about the reason for such a messed up project. Perhaps, if Benford's Law was applied to the data for all UST holders, Genesis Trading might not have swapped. Because no case in accounting does not follow Benford's Law, and it is legally used to catch fraud.

Sam Bankman Fried calls himself a practitioner of Effective Altruism and acts as if he doesn't care about his personal interests, donating to prevent a pandemic, or reviving a cryptocurrency project that has gone bankrupt due to a lack of funding. He reigned as a virtuous ruler in the industry, a white knight in the cryptocurrency industry. However, in addition to FTX, there were projects to create

trustworthy cryptocurrencies that were used in real-world services, but FTX, a group of malicious strongmen, chose deception. It was used as a hotbed of accounting fraud, resulting in billions of dollars in fraud. In 2001, Enron inflated its company value and tried to make it look like a sound business by receiving investment through fabricated accounting, but it was eventually caught and legally punished during verification with Benford's Law. But in 2022 something even dumber happened. FTX International received FTT as an investment from Sequoia Capital. Sequoia Capital, which was lucky to have a lot of money to invest in google and was famous for its extraordinary visions, followed SBF's words that it would sell bananas to FTX rather than verify accounting data with Benford's Law which had been used for 21 years, and threw `$21 million` into ignorance like a monkey trapped in a laboratory. Because no accounting case does not adhere to Benford's Law, and it is legally used to detect fraud. They all ignored the fact that the price of the tokens they own in the market changes as a result of market transactions and only made a false statement that the price was always constant or that the value would increase, and they did not disclose the distribution status transparently and issued tokens as they like, manipulating values to deceive people.

We must understand the true meaning of justice. The governance token currently determines the ruler, and the team member with the issuance right becomes the ruler, and there must be no justice for the strong who abuse their power. How long will we continue to praise these low-quality individuals and be used by contradictory rulers? The Standard Protocol recognizes that other cryptocurrencies, including the current project, have tokenomics that can be exploited in this manner, and specifies a method to maintain the Standard (STND) token's clear function and long-term value. From the time this white paper is published, the standard (STND) token will undergo implementation changes, revealing that it is a token that can acquire membership in all standard protocol services. Membership will alter the current DeFi governance structure and will be used to eliminate the pervasive Ponzi structure of decentralized finance. Services implemented based on this new governance and tokenomics are defined as DeFi 3.0. Justice ought to be about the strong being able to assist the weak by offering specialized skills, not about the strong having more tokens.

Tokenomics 2.0

Membership Token

Standard Labs, a developer of Standard Protocol, uses blockchain technology introduced in the information era. Thus, it has the mission of educating more people on the sovereignty of digital assets, developing software services that support sovereignty, and establishing and upholding a way of life-based on the importance of digital self-sovereignty in Web 3.0. As a result, users who use the service are classified as Standard members, and Standard (STND) will be used as a token to obtain membership and maintain status each year, generating continuous demand.

Value Parity

There must have been a case of using $600 per transaction while using DApps on the Ethereum network when the gas fee was high. When the cost of tokens for use rises, software built on a blockchain may become difficult to access for those who actually need to use it. The standard protocol, on the other hand, properly maintains the token value and the appropriate cost to perform the function, while properly distributing the token to those who require it. As a result, even if the token price falls, we propose a method to avoid speculation while maintaining the value of members' assets in a decentralized autonomous organization.

If the token economy must be inflated to equilibrate to a reasonable value, when the mainnet is created, we will increase the standard (STND) tokens paid to verifiers for block verification or allow them to purchase newly issued STND tokens with membership points each quarter. When it is necessary to shrink the token economy, the amount of standard (STND) tokens paid by verifiers when verifying blocks can be reduced, or the amount of standard (STND) tokens required for membership subscription costs can be increased. The Standard Protocol contributor members propose and vote on the agenda for all of these processes.

Proof of Membership

The membership provided by the standard protocol is aimed at eliminating the deep-rooted evils of privilege that VCs or developers have perpetually benefited, and tyrannical politics without legal boundaries, by simply holding tokens from existing DeFi project tokens without contributions in the decentralized financial system. Besides that, it enables the people to exercise their rights who actually use it the most and have the greatest impact on the DeFi project.

Standard Labs Corporation issues membership, and individuals who obtain membership have the following rights based on the characteristics of membership.

- The right to vote on issues related to the Standard Protocol as a member of the Standard Protocol decentralized autonomous organization (Digital citizenship)
- Privileged access to new services launched by Standard Protocol (Privileged Access)
- The right to exchange membership points for services or goods provided by Standard Protocol (Exclusive right to trade Standard asset with membership points)
- The right to transfer or trade membership to another person (Freedom of exchange)

Membership is given as an ERC-1155 **NFT**, and regardless of metadata, it can be proven that the membership **NFT** was issued in the standard protocol membership smart contract and that the membership **NFT** is in the wallet.

Subscription and Point

In order to maintain a balanced autonomous organization for operating the protocol, the standard protocol determines the protocol's direction with a temporary commodity called Membership Point (MP), regardless of the amount of tokens held. Membership is valid for one year, after which it must be renewed by paying standard tokens to the membership smart contract. Standard memberships may be applied in various ways, and each membership may have a different purchase price, subscription fee, points awarded at the time of subscription, and maximum subscription period. An annual new membership, for example, may cost 100 USDC to purchase, 2000 STND to subscribe, 50 points to subscribe, and a maximum subscription period of one year. However, in the case of the Genesis membership issued at the start of the project, the purchase price is 10,000 USDC, the subscription fee is 600 STND per year, the subscription points are 3000, and the maximum subscription period is 20 years.

Points are non-transferable points when a standard member subscribes and participates in standard protocol decentralized finance. For example, if a member understands the asymmetric key encryption algorithm of a cryptocurrency wallet on a standard protocol decentralized exchange and trades with the other party, issues a stable coin with an individual's collateral, or uses it for standard protocol internal contracts, the member is rewarded with points. Points can be used to vote as much as they are collected during each quarter set by Standard, and can be exchanged for digital assets or services provided by Standard Protocol each quarter. To illustrate, the standard protocol treats 360 days as one year in smart contracts, sets the accounting start date as January 1, 2023, and divides the year into quarters. User A joined and subscribed on March 1, 2023, earning 900 points in 2023 and 300 points after January 1, 2024. In this case, user A has 900 points of influence for 360 days beginning January 1, 2023, and 300 points of influence in 2024, and he can vote for each quarterly agenda by 900 points and 300 points. Each quarter, A can exchange the points accumulated at the end of the quarter for digital assets or services provided by the standard protocol. The goods that can be exchanged in each quarter will be detailed in the **New Order**, **SAFU**, which will be explained later.

Distribution of Wealth

The contributors of Standard Protocol are a group that prioritizes continuous profits obtained after building an economic system using blockchain technology rather than economic profits from cryptocurrency. This splits the revenue from all decentralized economic systems implemented by Standard 6 to 4 to maintain ongoing revenue and community ties. And each quarter, community members can exchange the remaining points of 4 for participating in the standard protocol. 6 is used by contributors to create new products to grow the pie and earn more money, or to hire new

contributors. However, 6 is proposed by Standard Labs and can be used publicly according to the community's decision. Examples of public use include:

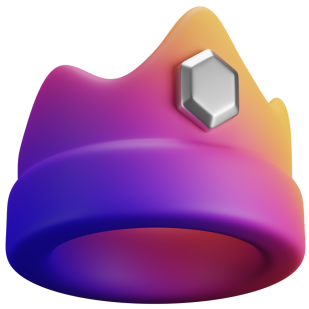
- Inviting a famous singer, not a superficial sociopathic "cryptocurrency" expert, to a blockchain event.
- Donating to non-political organizations
- We support the costs of class action lawsuits against coin-related victims to verify the authenticity of blockchain technology.

Every time, Standard's decentralized financial service is required to disclose how the user's fund is deposited and how the fee has profited.

Governance

In contrast to using existing tokens, governance is run through membership points issued annually. The agenda is voted on by governance, and the one with the most points is adopted. Voters receive points each time they participate in voting; they do not use points to vote on the agenda.

2. New Order



New Order is the first decentralized order book decentralized exchange to use a smart contract as a matching engine. Many people have attempted to implement a user experience similar to current blockchain exchanges, but no one has described how transactions are established. In the case of Vitalik Buterin, he stated that an order book exchange could be implemented5 by hastening blockchain transactions with plasma, but the idea was merely speculative and never materialized. Vitalik simply avoids describing or specifying how blockchain stores digital assets as a third party, simply stating that zero-knowledge proofs can solve everything by introducing them pathologically,

as zero-knowledge proofs solve everything. It should go without saying that zero-knowledge proof is a privacy-protection technology. It is unacceptable to use it to demonstrate knowledge when you lack expertise in any field. How will a program that can make pre-sales based on zero-knowledge proof be validated? Didn't SBF bring Serum from Solana because they said speed was crucial?

An attempt was also made to move the order book to layer 2. The Dy/Dx project, like the previously described plasma, stored transaction order data in the blockchain and processed purchase and sale orders using an external server, but the transaction itself was impossible due to Amazon Web Service server failure. If only the external server has limited access to the user's deposited order and processes the asset by matching it with other orders, the external server's manager can create a sell order and match it to the user's buy order to steal the asset. This is not decentralized finance because Dy/Dx users are effectively handing over ownership of their digital assets to Dy/Dx with no restrictions and leaving it entirely up to them. Polkadex, another layer 2 order book decentralized exchange project, claims to use a Trusted Executed Environment (TEE), but it is actually more malicious than Dy/Dx. At the very least, Dy/Dx stated that the matching engine, which it refers to as "Layer 2," is the server, whereas Polkadex is a closed blockchain that only appears to be a blockchain, so if the project team removes the encryption key to view the matching engine, you won't know what they did. When you use external clients to manage users' deposits, the proof of solvency that can return the user's deposits becomes ambiguous, and personal asset ownership is never guaranteed. Are they claiming that they learned nothing from FTX?

New Order is a decentralized exchange created by Standard out of the Uniswap Fork used in Standard 1 last year. **New Order** is an order book exchange that was created in response to issues with the existing Uniswap algorithm, and unlike centralized or sub-centralized exchanges, all transactions are processed within Blockchain without compromising centralization. A smart contract, in this way, completely prevents the embezzlement of the user's deposit.

Limitations of AMM

The Uniswap Fork that made it possible to buy and sell stablecoins in Standard 1 was problematic. The introduction of StableSwap like curves was attempted a year ago, but essentially an autonomous market maker (AMM) proved problematic. This is because it is more appropriate to think of it as a Forced Market Maker, which does not operate autonomously but is forced to operate at a price set by 10% of liquidity providers.

AMM has several variants, but they all come from Uniswap. Uniswap is a decentralized exchange (DEX) that enables automated exchange transactions between Ethereum and ERC-20 tokens, and asset suppliers to Uniswap, also known as liquidity providers, are necessary for asset trading.

In this white paper, liquidity provider is abbreviated as **LP**. **LP** supplies assets in exchange for a fee of 0.3% of the imported assets when users exchange assets each time, and Uniswap determines the rate at which one asset can be exchanged for another asset by the number of assets supplied by this **LP**. The polynomial that determines this is determined as x*y=k. In V1, only token exchange between Ether and other ERC-20 was supported, and in V2, other tokens were also supported, but **LP** had a problem in that it had to be supplied to a pair that wanted to exchange two assets at the same time. However, V3 has overcome this challenge and solidified its position as the market's representative decentralized exchange.

However, the liquidity provider's formula, x*y=k, does not reflect the demand for future value for all digital assets. In anticipation of the future, buyers and sellers cannot decide to buy or sell at a price higher or lower than the market price. This is because the asset's value is determined by the **LP** that supplied the most assets to each asset pair. If you want to change the price of an asset in Uniswap V1 and V2, the **LP** that supplied the most assets can withdraw the stored digital assets from each asset exchange contract and set it to the desired ratio. V3 counters that this problem can be avoided because only one side can be supplied; however, to receive a 0.3% commission, one side can only be supplied at the price that supplied the most **LP**s. If this is not followed, an **LP** that can supply more assets may change the price, and it may cause losses by those seeking arbitrage trading between exchanges. Then, it is best to find a place that provides the most asset liquidity throughout this market and matches the price, but where is that? On the centralized exchange (CEX), assets are being supplied and traded with far superior liquidity than Uniswap! After all, with this structure, Uniswap has no choice but to match the price of a centralized exchange!

Anyone, regardless of asset or position, should be able to trade an asset at the price they offer in a free market. However, decentralized exchanges only function for users to trade, but they are designed to trade only as they set by adhering to the **LP**'s price. This, like North Korea, is a planned economy designed by a small number of **LP**s. In a free economy, how could you possibly do this? It is a planned economy in which innocent individuals must supply or buy their assets at the price set by the **LP** in accordance with those who previously supplied them. In an era when abnormalities are frenzied to enter the normal category, how long will we be playing with the puppet show that advocates socialist agenda-like decentralization created by them? AMM like Uniswap may compete to become the most efficient secondary market exchanges, but they will never be defined as free market exchanges that determine asset value in a decentralized manner.

Proof of solvency

Standard Protocol's decentralized financial software, **New Order**, describes how users' balances are protected and how fees work. First, unlike the software used by other centralized exchanges, **New**

Order does not support partial payment. This is because it does not deposit or withdraw cryptocurrency. Second, it is in charge of and has operational authority over all orders in the **New Order**.

New Order, unlike Binance, does not compromise on fractional reserves. If the user's deposit is operated, a smart contract is created and approved with the user's private key before proceeding. No matter how well-prepared a Merkle tree is, the background does not contain approved data that allows users to use their deposits in the name of the exchange, and the record of using the deposits cannot be tracked.

Individual users in **New Order** have complete operational control and ownership over their actions regarding the selection of all transactions supported by the exchange platform. Furthermore, unlike other centralized exchanges, **New Order** does not charge withdrawal fees when assets are withdrawn from the exchange. This is because users already have all of their digital assets stored in their wallets. If your cold wallet supports electronic signatures, you won't have to worry about exchange hacking and can instead focus on keeping your wallet safe. If a hacker wants to hack the **New Order**, he must first hack as many cold wallets as there are users. Even if Standard Labs' wallet is hacked, it will only take the fees paid to operate the exchange.

New Order moved functions previously provided by centralized exchanges to smart contracts and implemented all matching processes in algorithms to prevent pre-sale. Now, users can use the order book exchange on their own without restriction using their cold wallet and have complete control over all transactions. The user's deposit is never lost, and the process of placing and canceling orders is entirely determined by the user, with all arbitration taking place in the smart contract. One order only costs about 230,000 Gwei to process. **New Order** also attempted to provide **NFT**s for order ownership in accordance with EIP-5252, but the current gas cost exceeds about 400,000 Gwei and is not competitive with the gas costs of other decentralized exchanges, so it is on hold.

Orderbook

The data structure of **New Order** consists of two linked lists for matching priority between buy and sell orders and two linked lists to save orders with its indices.

Price Linked List

The order book eventually receives orders and makes a list so that the order to sell at the lowest price in the case of a sell and the highest price in the case of a buy are processed first. Accordingly, when a buy or sell order is received, the **New Order** retrieves price information and compares the order by

arranging the price of the order in the existing linked list. If the price of the buy order received from the user is the highest, it is placed in the head if the price is the highest. Afterwards, when matching, the price to be matched is called from the linked list by `front pop` operation. Until the corresponding price storage becomes empty, the matching engine repeats the same operation.

Order Storage

When the price to be matched is called from the smart contract, the order is fetched from the order storage where orders to be processed for each price are stacked. The storage of sell/buy orders consists of one mapping in which the key is price information and the value is a linked list hash map for orders, an order mapping that stores orders as a whole, and a head mapping that stores each order index price as a head value. For each order, a linked list is formed whenever a price is newly created, and in order to minimize the amount of memory used to load the order structure data each time a match is made, the more funds deposited, the higher priority is placed in the list to be processed.

Adding Trading Pairs

New Order, like Uniswap, allows users to freely create new assets. Unlike Uniswap, it has separate pools for each base currency and relative currency, taking into account the demand for each asset. In the case of **ETH/BTC** or **BTC/ETH**, for example, each is operated as a separate smart contract, and the number of assets that can be exchanged may also differ. The matching engine stores address information about pairs, and **10000** Standard (**STND**) is required for each addition to prevent spam that adds asset pairs indiscriminately.

Limit order and stop order

A limit trade matches orders from the stacked order storage at each price until a price is greater or less than the price specified in the linked price list. Market price trading continues until the user runs out of assets to buy/sell deposited in the smart contract. The gas fee is used more frequently as the number of times the order is matched increases, so use it with caution. A stop order is an order that is placed at the market price when a certain price is reached. Without regard for matching, stop orders are simply prioritized based on the amount deposited in order storage for each price.

Complexities and Optimization

If the order book is implemented in the current EVM, approximately **400** orders at the basic gas limit for each price could be placed repeatedly. The most expensive gas was about 1.2 **ETH**.

Implementation

The implementation is currently implemented as a solid smart contract, and implementations will be expanded in the future.
The links below are the implementations that are distributed and managed in each blockchain and will be added as they are continuously uploaded in the future.

- EVM
- NEAR
- Cosmwasm
- Move
- Substrate Runtime

Distribution of Profit

Scoring and Rewards

Score Measurement:

- 10 points for each pair added for each/specified asset
- 10 * (amount of trading asset * market price in trade) points for each order matched for each/specified asset

Rewards:

- Achievement Soul bound tokens which measures points every quarter and allocate more points on each financial year.
- Dex's profit, The fee which can be claimed for all asset in reward from one membership point is (total fee locked)/(total supply of membership point)

- When Standard is issued, newly issued tokens can be exchanged with points.

3. SAFU

SAFU is a decentralized stablecoin linked to the **New Order** beyond the limits of **USM**, which was used in standard 1 oracle or liquidation using **AMM**. The ticker is **SAFU**, and the decimal is set to 8 considering the decimals of WebAssembly and other blockchain tokens. As for the issuance method, users generate **SAFU** stablecoin by depositing collateral in **CDP**. Following that, the IOU is received as an **NFT**, and **SAFU** stablecoin on the collateral, and IOU smart contract can be issued and incinerated by the user later.

SAFU Stablecoin can be distributed within Blockchain under the same name, and to deter fraudsters who use this to launch Token spoofing attacks, the **SAFU** Token address is revealed in the above white paper whenever a **SAFU** Stablecoin address is created. The **SAFU** stablecoin implementation address varies by Blockchain and will be added as a Source of Truth to this white paper whenever Blockchain is supported.

- Smart Contract

Network	Address

- Native Coin

Building Decentralized Reserve Currency on Web3.0

SAFU functions as a decentralized reserve currency in Web 3.0 with the following four properties.

1. `Measure of Price` : Any digital asset's value should be able to be measured with the currency's exchange activities which is domintantly determined by inconvertible notes or fiat money.
2. `Store of Value` : One must be able to store money safely and with guaranteed ownership.
3. `Means of Exchange` : To maintain exchange at a stable price in comparison to the fluctuating value of digital assets, a mechanism is required to prevent inflation/deflation.
4. `Payability` : It must have solid liquidity position to exchange with other digital assets to function as stable payment gateway.

1. Measure of Price

Currently, stablecoin projects rely on USDT or USDC as there is no price scale to create a decentralized economy. In China, starry clams were used as currency, and it was common to find shells or stones used as currency among Pacific Indians. It is known that salt was used as a medium of exchange in Abyssinia, shells in some parts of the Indian coast, dried cod in Newfoundland, tobacco in Virginia, sugar in some parts of the West Indies, and rawhide in others. If you set a currency with a stone, you can just pick up a stone, but when you set a cryptocurrency as a currency, you have to create a computer, write software on it, connect it to other computers and networks, and go through more trouble. But why is a stone that can be easily picked up from the ground easier to set as currency? That's because the stone is a measure of price and people can negotiate and set prices.

When a stablecoin is used as a price measure, the **CDP** between the stablecoin and the collateral used at the time of issuance is calculated upon liquidation. **USM** believed that if MakerDAO liquidated the stablecoin **CDP**, the auction system artificially set up by the protocol manager would appear to be a planned economy, so it would bring AMM and liquidate it to keep prices stable with the stablecoin and collateral. It was because AMM was deemed to be a decentralized method of setting prices at the time. AMM was supposed to automatically determine the optimal supply and demand based on the market economy, but the reality was quite the opposite.

It was designed with the assumption that liquidation would temporarily raise the price, and that one day someone would arbitrage and normalize it to `$1`, matching the price of `$1`, and the price of any digital asset would stabilize. However, contrary to this assumption, arbitrage has caused problems. The liquidated collateral in Uniswap created a spread that is difficult to compare with any other exchange. Creating such spreads resulted in a toxic order flow, further complicating asset trading. Maintaining stablecoin prices is difficult when the price of stablecoin changes from **1`.2** at **$600** volume.

Replacing AMM with a curve was also considered, but as previously stated in the context of creating **New Order**, the curve's `x+y=k` automated liquidity formation did not solve the problem. Although setting the price arbitrarily is convenient, it can be abused to keep the price stable if a certain amount of asset liquidity is supplied. Experiments on decentralized exchanges using algorithms like real curves have revealed that, although the value of `$1` is not maintained, some of them are traded at `$1`, which is surprising. Terra/Luna's price was able to maintain a peg at `$1` on decentralized exchanges like Curve until asset liquidity was subtracted, which made people feel complacent about Terra's value. This is effective in maintaining the price of the stablecoin, but in order to maintain it, it is like cross-trading the stablecoin at the price you set. In addition, the formula that forms the pair of

Curve changes the price rapidly when it is outside of a certain range, so it is inappropriate because the price changes rapidly when listing an asset with insufficient liquidity indiscriminately.

Through **New Order**'s order book, **SAFU** collects spreads that allow stablecoins to exchange collateral for `$1` . Upon liquidation, **New Order** places a limit order until the stablecoin's price in the corresponding collateral pair reaches 1USD, buys and burns the stablecoin, and places a stop order so that the remaining collateral can be sold when the stablecoin's price reaches `$1` . This makes price defense more stable in the event of a future sell to break the peg and narrows the spread at a price where the stablecoin's value is set at `$1` after several liquidations. As a result, a price that enables stable transactions between stablecoins and collateral can be established. By using each random digital asset as collateral and repeatedly liquidating it, a stable price scale that can be purchased for `$1` is established.

Liquidator

The liquidators liquidate Stablecoin's **CDP** if it is insolvent. When one subscribe to a membership, one can join them and liquidate the positions. They will be rewarded with membership points. They are the operator that evaluates the collateral connected to the currency and adjusts liquidity where the asset can be traded at the correct price where **SAFU** can be traded with one dollar price on **New Order**.

2. Store of Value

Proof of Reserve

When borrowing stablecoins, **SAFU** abstracts accounts into **NFT**s, allowing borrowers to manage both collateral and stablecoins. The reserves are solely allocated to the user's contract, and the user has its full control. This prevents DeFi hacking and protocol managers from running individual assets without permission. When a debtor opens a stablecoin **CDP** (Collateral Debt Position), for example, an **NFT** called Vault and an issued **SAFU** are issued, and the **NFT** called Vault represents an account that can manage **CDP** and be moved to another wallet. This means that debtors can use stablecoins as well as sell **NFT**s by treating them as bonds. Furthermore, by using the **CDP** account, the debtor can even exchange the collateral with consent for another asset. With these systems, it ensures that ownership is guaranteed on the blockchain, making it secure and capable of storing money.

3. Means of exchange

Pegging mechanism

For **SAFU** to act as a smooth means of exchange, liquidating the **CDP** may not be sufficient. If the measured price is not maintained, for example, when liquidation does not occur in time or the price of digital assets that can be paid to one **SAFU** falls sharply, the economy should contract, and in **New Order**, the economy should expand when **SAFU** trades at a price higher than $ 1 and trading volume is significantly lower.

Interest rate

SAFU's **CDP** has an interest rate. As the interest rate increases, **SAFU**'s liquidity decreases and it speeds up the recovery of the price of `$1` . As the interest rate is lowered, the liquidity of **SAFU** increases, but it becomes difficult to maintain the price of `$1` . The interest rate keeps inflation and deflation at bay.

4. Payability

Overcollateralization

SAFU stablecoin are usually issued with the overcollateralization rate initially set at 300% for any token except fiat-backed stablecoins or CBDCs. As liquidation occurs and the spread of orders are adjusted at `$1` is concentrated, Overcollateralization ratio can be decreased. The Overcollateralization ratio is determined around the value of (half of the token's total circulating supply) / (circulating quantity piled up in the order trading at `$1` price of **SAFU**). After going through the price measurement process, collaterals are converted into assets that can be paid with **SAFU**. **SAFU** will achieve payability to other digital assets by accomodating digital assets to be collateralized.

Implementation

The implementation is currently implemented as a solid smart contract, and implementations will be expanded in the future.
The links below are the implementations that are distributed and managed in each blockchain and will be added as they are continuously uploaded in the future.

- EVM
- NEAR
- Cosmwasm
- Move
- Substrate Runtime

Distribution of Profit

Score Measurement

- √x points when x is the number of stablecoins issued.
- √x points for liquidators when x is the market value between liquidated assets and **SAFU** at the time of each liquidation

Rewards

- Achievement Soul bound tokens which measures points every quarter and allocate more points on each financial year.
- Dex's profit, The fee which can be claimed for all asset in reward from one membership point is (total fee value)/(total supply of membership point)
- When Standard is issued, newly issued tokens can be exchanged with points.

Conclusion

The origins of cryptocurrency can be traced back to the fact that blockchain technology can protect assets under one's own responsibility, and on top of that, independent individuals can now determine their own value while conducting economic activities without the assistance of an existing arbitrator. However, the current cryptocurrencies do not define themselves by the justice they represent. Through blockchain technology, more individuals will be able to transact on behalf of trust with more people safely and transparently, and arbitrators who say justice is for the strong will be eliminated, allowing their value to be properly evaluated. Standard will create and maintain a democratic monetary system software that will create arbitrators whose justice is that the strong contribute by providing technology to the weak.

Standard 2.0 is developed to eliminate the arbitrators mentioned in this. In contrast to existing token holders who were strong, the new tokenomics allows the person who contributed the most to maintain Standard to become the strong and receive a fair price and govern Standard. In **New Order**, the person who contributed to trading digital assets at an appropriate price on the decentralized

exchange, where the person who spent the most money and provided the most liquidity in determining the price, becomes a strong person in conjunction with tokenomics, allowing the value of digital assets to be determined transparently. **SAFU**, a stablecoin based on this, supplies stablecoins to StableSwap decentralized exchange called Curve, which maintains the price of existing stablecoins to some extent regardless of asset liquidity. We will correctly evaluate the collateral assets by changing the system where people who take **LP** fees were the strong, and by correctly evaluating the assets backing the stablecoin, we will ensure that contributors to the creation of the stablecoin can pay with those assets and increase the number of assets that can be transacted transparently. It is hoped that these technologies will create a fair and democratic society in which the strong will contribute to the weak in the new Web 3.0 era, without relying solely on false gods or idols that govern for nothing.