X|SIGMA

xSigma DeFi Whitepaper

Last updated: January 12, 2021

Market Overview

In 2008, new cryptocurrency Bitcoin emerged as a solution against centralized money printing. By 2020, Bitcoin market cap reached 700 billion USD. Bitcoin is a decentralized, trustless database that stores all transactions in an immutable manner and only allows editing with strict rules. Bitcoin's main appeal is that it can replace centralized authority and provide control without authority. For many, this makes it a new digital gold.

In 2015, Vitalik Buterin launched project Ethereum. The main difference between Ethereum and Bitcoin is that the latter is not a database, but a decentralized computer. Ethereum can not only store transaction data, but also store and modify arbitrary information. This allowed a vast range of applications, starting with ERC20, which is basically a blueprint for self-hosted units, called tokens. This continued into Kickstarter-like apps, prediction markets, games, loan and borrow protocols and decentralized asset exchanges. This marks an improvement on Bitcoin's idea of replacing traditional banks in this role.

DeFi, which stands for **De**centralized **Fi**nance, aims to build a system which can work openly, securely, and in a modular manner, so that anyone can join it, use it, contribute to it and upgrade it. The main idea is to recreate financial services and tools that are entirely on blockchain, eliminating the need for banks or other third parties as intermediaries. This makes it fast, inexpensive and available to everyone. Further, the open-source nature of DeFi makes it transparent and trustless.

A chicken-egg problem has emerged as a stumbling block along this path such that people could not use certain new products because there was insufficient liquidity, meaning insufficient resources locked in the protocol. For example, if an exchange platform wishes to enable a swap of ETH into a token using a decentralized exchange hosted on the Ethereum blockchain, the exchange would normally require sufficient tokens to process the request. Similarly, we would not expect a user to provide their tokens to be locked into the exchange if there are no users who want to buy and sell them.

In 2018, Uniswap applied the concept of an automatic market maker (AMM) by which one party provides liquidity. In this environment, the liquidity provider (**LP**) is compensated so that their liquidity is used as the basis of trades occurring on the platform. All LPs are in an equivalent position, in the sense that they all earn in proportion to the liquidity they have contributed, each benefiting in identical terms from application of the formula of the AMM.

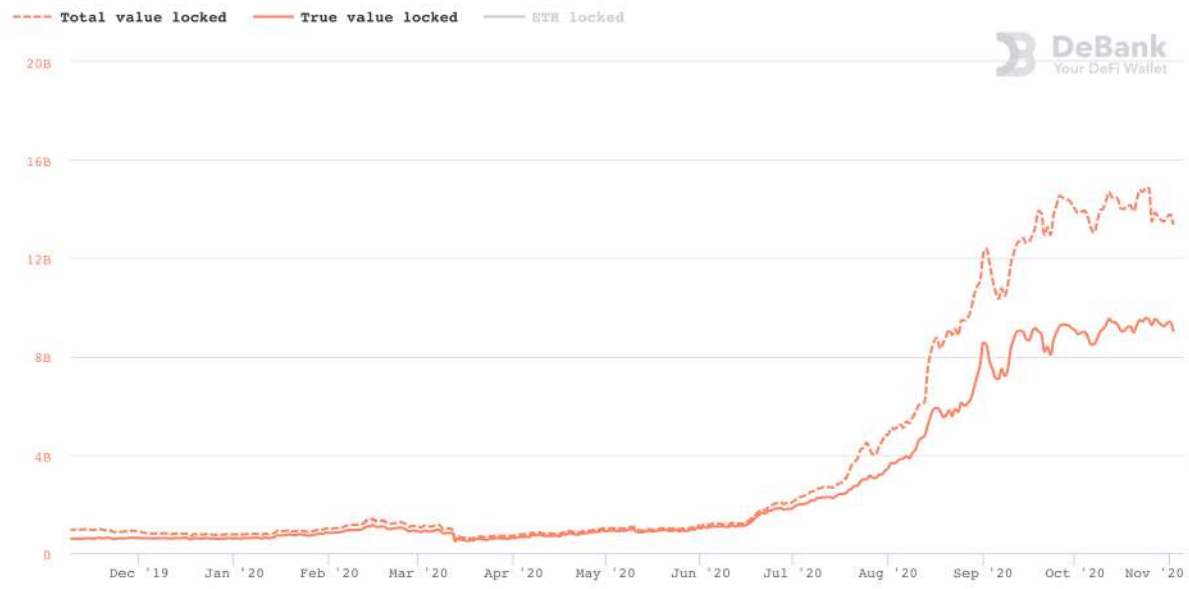
Uniswap grew such that in August 2020 it reached a higher daily exchange rate than Coinbase – the largest US-based crypto exchange. This spawned a new DeFi trend, focusing not only on users, but also on LPs helping the latter earn consideration by contributing to the success of the system.

From this, new products like lending/borrowing platforms (Aave, Compound) emerged, with some even allowing for margin trading or shorts trading.

Curve is an exchange that built a special-case AMM which uses only stablecoins (coins that are pegged to a fiat currency, typically $1.00 USD) and price knowledge. Participants do not expect much variation in the price of a stablecoin because it is pegged to a fiat currency on a 1:1 basis. Using a special formula for price changes in AMM, Curve appears to provide better price slippage and lower impermanent loss, resulting in better consideration to LPs than the Uniswap algorithm in the same situation.

To date, Curve has also been a success, with $2.6 billion in daily turnover and $1.3 billion locked in the platform as of this publication.

Despite a drop in hype, the DeFi market as a whole has been on the rise: growing to $14 billion locked, as per debank [1].



[1] https://debank.com/ranking/locked_value?chart_date=1Y

Problems with Current Solutions

Despite rapid DeFi growth, the incumbent platforms have not solved several key issues.

ETH Transaction Fees

The biggest problem is Ethereum scalability. The volume of participants joining DeFi platforms has driven transaction prices to an all-time-high, sometimes as high as $10 to $50 per transaction. This problem is being addressed by several developers, including Buterin himself who is working on Eth2.0 and Layer-2 solutions.

Governance

Another problem comes from what can be called the 'trustless two-sided sword'. If there is no central authority, then there is no person to arbitrate between right and wrong. A leading solution to the problem of governance in DeFi is decentralized governance whereby decisions are controlled by participants in the platform who are usually holders of platform-specific tokens. This system is called a decentralized autonomous organization (**DAO**).

While this is a clever hack for introducing some governance into an otherwise immutable and lawless platform, the DAO itself is imperfect and presents some issues.

Critically, DAOs are not impervious to hacks or the bad acts of founders. Depending on how the DAO operates, it can allow voting for certain issues, but the founder team, being human, may be corrupt. Corrupt founders with control of the DAO can corrupt the proper and faithful implementation of decisions voted upon by platform token-holders. This reality creates an imbalance of power between founders and users that is awkwardly reminiscent of centralized finance.

For example, the DeFi SushiSwap DAO had a 100%-community fair launch. Not very long after launch, the founder dumped all of their tokens, crushing the token price and endangering the whole platform[1].

Despite the DAO's promise of trust-without-trust, governance problems persist. Excessive concentration of governance tokens of the DAO, being tokens that carry the right to vote for changes on the platform, render the DAO somewhat similar to a centralized platform; the holders of, for example, a majority of tokens, could vote in their own favor. Therefore, the DAO governance token has to be distributed widely enough to avoid being just another centralized platform. Wider distribution also prevents coordinated selling of governance tokens that would artificially impact price, as was the case with SushiSwap.

Legal and AML Compliance

Most DeFi platforms provide no terms of use, even for their website front-ends, and do not appear to make efforts to limit the abuse of their platforms in sanctioned jurisdictions.

False Promises of High Returns

Some DeFi platforms promise annual rates of return that are absurd, such as 100% or even 200%. These promises, even if true, are true for the tokens of the platform which, themselves, are subject to fluctuation in price, potentially wiping out the would-be gains. Ironically, as the price of the platform tokens increases, there are correspondingly less issued to LPs thereby further eroding the would-be gains. This phenomenon has been observed in stablecoin-based platforms, such as Curve.

High Barrier to Entry

Higher transaction fees on the ETH blockchain mean that the rewards of locking-in liquidity need to be correspondingly higher to make it economically reasonable. The result has been that for any LP placing less than $5,000 or $10,000 of liquidity into

[1] https://coinmarketcap.com/headlines/news/sushi-token-holder-dumps-defi/

the platform, the transaction fees are likely to be greater than the reward, thereby creating a barrier to entry for smaller LPs.

User Interface (UI)
DeFi platforms are often difficult to understand for users who are not programmers. Indeed, it is surprising that some of the other platforms have actually secured billions of dollars worth of liquidity despite being essentially impenetrable by ordinary users.

Anonymous Shadowy Founders
The founders of some DeFi platforms, such as Swerve, have opted to remain completely anonymous, which poses challenges for a compliance and risk perspective, even in the world of DeFi because users cannot look to anyone if they have questions or concerns about the platform.

Our Solution

Our solution presents improvements on existing platforms with respect to those elements of DeFi that we believe can be improved, as discussed below.

User Interface (*UI) — User-friendly*
With xSigma DeFi, we offer simple clear UI, that appeals to banking and investing metaphors, already known to the users. Without misleading LPs into believing anything false, xSigma uses commonly understood concepts to connect users with its platform.

Founders — Known to All
The majority owner of xSigma is a public company that we expect will give our users a base-level comfort of a public responsibility for team actions.

Legal and AML Compliance
By definition, it is not possible to perform know-your-customer (KYC) on every user of a decentralized blockchain. Other DeFi platforms appear to use this as an excuse to do nothing at all. We take a different approach. We will not control the Ethereum blockchain nor will we control our protocol at a certain point following launch. We do, however, control our own portal through which many, if not most, LPs and others are likely to access the xSigma protocol. Taking advice from U.S. AML legal counsel, we have decided to add layers of protection in those areas that are reasonably within our control.

The front-end website is subject to terms of use as well as a privacy policy. Other DeFi platforms have no terms of use and no privacy policy. It is a fallacy to believe that because one's portal enables access to a decentralized protocol that the portal itself is somehow unaccountable. xSigma makes no promises as to the performance of its protocol or the related governance token, SIG. xSigma is not accountable for performance of the protocol, as it is a public, transparent protocol against which any LP or other user can post transactions. However, xSigma does control its own portal that will be used by many LPs and others. Within this narrow spectrum of control, xSigma takes responsibility subject to the terms of use posted to its portal.

Given that xSigma does not control user wallets or LP assets, users are able to remain true to the core principles of DeFi while also taking comfort in knowing that the front-end of the platform is provided pursuant to reasonable terms of service.

Critically, to combat money laundering and the financing of terrorism, unlike other DeFi platforms, xSigma blocks IP addresses in specific jurisdictions and takes other measures to decrease the likelihood of the xSigma platform being abused by bad actors.

To the extent xSigma is capable of gatekeeping access to its platform via its front-end website, it takes action to filter traffic from known bad-actor sources.

Proven Formulas

xSigma is built on top of the Curve/Swerve swap mechanism[2] with a view to improve them. The xSigma proposes slippage cash-back with token burn, which is discussed below. To the extent that Curve/Swerve are flawed, however, xSigma will be similarly flawed in terms of its core code.

DEX Fees

Most crypto exchanges charge a fee of up to 0.30% on transaction volume, xSigma takes 0.24%.

ETH Transaction Fees Avoided for Some Governance Items

xSigma proposes to use some off-chain governance for preliminary proposals, specifically where fee-saving is necessary for the governance item.

[2] https://www.curve.fi/stableswap-paper.pdf

It is our hope that all of our competitive advantages may provide us with solid market share in the fast-growing DeFi market of the stablecoin exchange niche. We do not promise that there will be any minimum volume on our platform. Below, we explain in slightly more technical terms, the above advantages of xSigma.

Token Utility

The xSigma governance token is called 'SIG' and has no intrinsic value. xSigma specifically renounced any representation or warranty as to the value of SIG. Instead, xSigma has programmed its DeFi platform to interact with SIG as a utility token, with the uses indicated below.

The SIG token has four use-cases

- DAO voting: Holders are able to use SIG to cast votes on certain decisions with respect to xSigma. None of these votes, however, can disposes LPs of their assets placed on the platform. No matter how SIG tokens are voted, LPs cannot lose the liquidity they have placed into the protocol.
- Claim of a part of DEX exchange fees: Holders of SIG earn fees as a function of the then applicable rules of the platform as coded therein. Please see the buyout and burn paragraph discussions above.
- Ethereum transaction gas cashback: Holders of SIG People owning SIG may receive a gas subsidy by some of their gas being returned to them on some platform transactions.
- Farming bonuses: Holders of SIG may earn additional farming bonuses as and when the platform elects to pay them.

Tokenomics

As with most DeFI platforms, xSigma has a DAO. Every holder of an xSigma governance token is eligible to vote on some proposal. Creating a proposal requires locking a certain amount of tokens. Proposals such as changing transaction fees, or LP rewards, or any parameters of the system are eligible for adoption only by reaching quorum of at least 10% of token holders and should be active for at least 2 weeks.

The name of the xSigma governance token is **SIG**, which is a short form of xSigma protocol. The purpose of SIG is to serve as a governance token and not a unit of exchange or currency. We specifically renounce any promise as to SIG having or gaining any real value.

The rules set out below are incorporated into the xSigma platform.

As liquidity providers, users can provide their funds to the exchange pool of the xSigma protocol. In consideration of liquidity, the protocol is programmed to generate rewards for LPs in the form of fees. Half of fees are returned to the pool, and the rest are spent on the buyout and burn of the SIG token.

In addition to fees all LPs also receive SIG governance token as bonus in direct proportion to the amount of liquidity they provide to the platform.

SIG is continuously minted. Rewards with 50 SIG tokens are minted in each block by default, and then halve every 210,000 blocks. This replicates Bitcoin mining policy to appeal to crypto users but works 40 times faster (as Ethereum blocks appear every 15 seconds instead of Bitcoin's 10 minutes). This way, xSigma halving happens every 36 days. Minting speed is a subject to change by DAO voting and can linearly change anywhere from 1x (default speed, reward per each Ethereum block, which is approximately one in 15 seconds) to 40x (Bitcoin speed, every 40 Ethereum blocks, once per about 10 minutes).

There is also a bonus for the first two weeks after launch. During the first week the minting happens at double (2X) speed. During the second week, minting happens at one and a half (1.5X) times speed This element of the DeFi protocol is designed to incentivize the early adopters.

We expect a total of around 24 million SIG tokens after full mint. 24,024,024 to be exact: 21M from the Bitcoin-like minting, 3,014k for the bonuses and 24 for the technical purposes.

Token Distribution

On minting of tokens in each block, they are distributed in the following proportions:

- 60% to current LPs who hold funds in the xSigma pools or in the SIG/ETH pool. In the first two weeks more rewards will be received in the xSigma stablecoin pool;
- 30% to the research and development and investors fund;
- 10% is locked into a growth fund. xSigma determines where these tokens are used, for purposes such as rewarding power users, influencers and early adopters or other project promotion and marketing expenses.

This distribution has no hidden pre-mint[3], no private early mining, is completely public and trusted, and is aligned with xSigma's commitment to maintaining transparency. The fair launch will be scheduled well beforehand, so those interested in participating will have sufficient time to prepare.

Swap Subsidy ("Cashback")

In order to attract users, xSigma will subsidize traders, so they receive cashback to cover a part of the transaction gas fee.

The exchange function in the smart contract automatically gives cashback to cover a portion of the gas used. The funds for that come from a separate depositary. This depositary is initially funded by xSigma, and in the future it will be funded from the growth fund. The cashback rate will be automatically adjusted according to the smart contract formula *min(avaliable_funds_to_the_date/10, max_cash_back)*level/10* where level is 0...10, based on how many SIG users possess in their balances. No staking is needed.

This will ensure that xSigma has enough users to build up a platform. Afterwards, it will have a flywheel effect where bigger liquidity generates better rates, and better rates attract more users to host more exchanges.

[3] except for the first block premint of 24 SIG for operational purposes

Buyout of Burn

xSigma uses the exchange fees fund to burn SIG tokens forever. Every term of 105,000 blocks (or about 18 days), half (½) of all accumulated fees to date are used to market-buy SIG tokens on Uniswap. Both term size and fee percentage to burn are subject to change upon DAO decisions.

This works as a two-way engine. The purchase of a large amount of SIG raises the market price with stablecoin fee fund. Then, xSigma burns a part of the SIG token supply forever, reducing token supply. These two effects combined might work to potentially raise token value for holders. That said, we do not promise that SIG will ever have any value, as its intended purpose is to serve as a utility for voting on DAO decisions of xSigma.

This approach might create additional ongoing demand for the governance token.

Advertising

xSigma intends to use the following methods to bring awareness to its protocol:

- Technical and promotional content generation, including blog and social medias
- Website SEO oriented towards DeFi
- Social media influencers who are engaged to disclose truthful information concerning xSigma without promises as to return on investment or inherent value in SIG
- Public Relations. xSigma will reach out to relevant blockchain media to tell xSigma's story and its latest updates.
- Paid advertising. Includes ads on Facebook, Google and banner ads on various blockchain websites.

Those who promote the platform will not be compensated as a function of the value of SIG.

Conclusion

xSigma is a decentralized stablecoin exchange with a clean UI, exchange subsidy and SIG tokens. Working according to the above rules, we expect xSigma to be a stable and attractive option for LPs that are shopping for transparency and stability in the DeFi market.

Disclaimer

For better or for worse, most of the operation of the xSigma platform is immutable following its publication to the ETH blockchain. That means, xSigma, as a developer of the code, has coded it, but afterwards xSigma does not retain control thereof.

xSigma cannot recover any stolen funds or can't re-deploy to fix bugs. As to the security of the liquidity provided to the xSigma platform, the user does not need to rely on the security or honesty of xSigma; the LP need only trust the code of the platform, which is published for anyone to review or audit.

The xSigma DAO governance token, SIG, is not listed on any stock exchange nor has it been approved or sanctioned by any government licensing or registration bureau. Your ability to acquire, control and dispose of it are published to the Ethereum blockchain in the form of the xSigma protocol and you are free to engage with it as you see fit subject to laws applicable in the jurisdiction where you are located.

Users must keep their private keys in a secure manner, as the private keys to their own crypto wallets are what control the liquidity they place on the platform. xSigma cannot access that liquidity or recover it if it is stolen or lost.

XSIGMA HAS PUBLISHED ITS PROTOCOL TO THE ETHEREUM BLOCKCHAIN; IT IS PUBLIC AND AVAILABLE FOR ALL USERS TO EXAMINE AND ASSESS. XSIGMA MAKES NO PROMISES AS TO THE OUTCOME OF YOUR INTERACTION WITH THE PROTOCOL. XSIGMA MAKES NO PROMISES AS TO THE ACTUAL OR EXPECTED VALUE OF THE UTILITY TOKEN 'SIG' THAT IS MINTED THROUGH THE PROTOCOL. XSIGMA IS NOT AN EXCHANGE, BROKER DEALER, BANK, MONEY SERVICES BUSINESS OR OTHER FORM OF FINANCIAL INSTITUTION. PRIOR TO ENGAGING WITH THE XSIGMA PROTOCOL, YOU ARE URGED TO REVIEW IT AND MAKE YOUR TRANSACTION DECISIONS ACCORDINGLY WITH THE ADVICE OF YOUR FINANCIAL AND LEGAL

ADVISORS. XSIGMA DOES NOT CONTROL YOUR CRYPTO ASSETS (E.G. ETHEREUM OR STABLECOIN); YOU CONTROL YOUR CRYPTO ASSETS AND ALL OF YOUR TRANSACTIONS WITH THEM INVOLVING THE XSIGMA PROTOCOL. XSIGMA IS NOT CAPABLE OF UNDOING ANY OF YOUR CRYPTO ASSET TRANSACTIONS.

Appendix A

Other Technical Features and Risk Parameters of the xSigma Platform

Impermanent Loss Risk Disclaimer for Pool2 LPs

Liquidity provided in the ETH/SIG on Uniswap is under potential influence of price change also known as "impermanent loss". More specifically, what happens when users provide liquidity for the pool, is that the user should stake equal market value of both assets: ETH and SIG token. Uniswap pool works by "constant product formula": pool_amount_ether * pool_amount_sig [before swap] == pool_amount_ether * pool_amount_sig [after swap]. Users who unstake funds when SIG/ETH price differs from SIG/ETH during staking should account that the market value of unstaked tokens might be less if the user had just held SIG and ETH tokens instead. This is true for absolutely any Uniswap pool (like ETH/DAI or any other) because of Uniswap's mechanics.

"No-risk" for LPs — Exit Strategy

Exit strategy for LP users: Users who provide liquidity for stablecoin pool receive pool tokens. DEX smart contract is able to exchange the pool tokens back for liquidity funds at any moment[4].

Range of How Much xSigma Pool Smart Contracts are Subject to Change

xSigma does not have any access to LP assets on the platform and is unable to alternate the code (smart contract is unupgradable) to grant them that access. Everything happens automatically, without human intervention on Ethereum blockchain by smart-contact execution. There's, however, the list of parameters which DAO can alternate within hard-coded constant limits, in this appendix.

[4] The stablecoins that you provide are converted to the pool share, thus you're guaranteed not a deposited amount, but a pool share. That means you may get a bit different stablecoins amount and proportions from the deposited. I.e., depositing 1000 DAI can give you nearly 990 pool share tokens, which in turn guarantees you approximately the same amount of USDT, DAI, and USDC totally worth 1000 DAI.

SIG created and distributed automatically — xSigma does not have access to and cannot change base and mint rate

- **Distributor** is a smart contract that is responsible for minting and distributing SIG token. It is based on the MasterChef open-source engine. Each block, some amount of tokens is allocated and is available for withdrawal. 60% of all the tokens created are allocated for LPs.
- During the first two weeks, mint rate will be hard-coded to give bonus tokens to the early LPs.
- Everything described here happens automatically on a blockchain smart contract.
- SIG token is a different smart contract from Distributor. It's un-upgradable and has a hard-cap limit onto minting speed. xSigma, as a developer team, can't change mint rate and total token supply.
- However, xSigma is an admin of the Distributor contract. While the rules for the first two weeks are frozen, we keep this admin privilege to be able to extend xSigma product further going into the future. Examples include adding other pools with newly created stablecoins, or tweaking reward distribution between pool1 and pool2.
- Note, however, that this is different from the pool smart contracts. The Distributor doesn't hold any user funds (i.e., liquidity), it only checks whether the token receiver is a LP and how much tokens it should mint.

Decentralized Features of xSigma

Voting, staking, reward distribution happens by trustless execution of smart contracts on Ethereum blockchain platform and voting count on https://snapshot.page.

So, here's a quick recap of how much xSigma as a developer is involved into the xSigma DEX Protocol:

- LPs keep the total control of their pool share. At any point, they are able to withdraw the total amount of stablecoins associated with the pool share she owns (i.e. their liquidity).
    - These rules are immutable. The smart contract controlling pool and pool-token is un-upgradable and xSigma can never modify the logic or interfere contract operation
    - The smart contract owner is an xSigma DAO, which is controlled by the SIG token holders.

- xSigma DAO is a full-scale DAO. Every decision it makes will only be possible with specific token voting mechanism
    - Research and development fund controlled by xSigma team receives the SIG token according to the immutable SIG issuance policy as everyone else, block by block. *The team doesn't have a way to create nor sell more SIG tokens than written in the smart contract.*
    - *The DAO voting mechanism would be fully integrated in the first two weeks when we expect the token distribution would be sufficiently decentralized.*
    - All xSigma decisions are public via this DAO.
- SIG token formula is frozen. There will be only ever 21 million + **3 million** SIG tokens. Ever. Period.
    - The only entity allowed to print SIG tokens is the Distributor contract. It prints them on request, but even it can't overwrite hard-coded rules.
    - The first two weeks of the token print won't follow the usual formula, but the rules they will follow are frozen already. They are immutable.
- Distributor smart contract admin is DAO.
    - DAO can add new pools to the Distributor smart contract and change pool weights in the reward distribution.
    - However, it can't change the total reward amount minted each block. It can only re-distribute the rewards between pools.
    - For example, it can vote to make pool 1 receive 90% of LP rewards and pool 2 10% or vice versa.
    - That means DAO can attack the system and even create fake pools.
    - However, the DAO holders are the same users who benefit from xSigma working smoothly, which ensures their alignment with project health.
    - While the DAO can change the rules over which SIG token is distributed between LPs, it can only do this publicly and with a delay of a minimum voting time. Also, it can't change distribution speed.
    - So, if the DAO changes the rules to something the community did not expect, they have plenty of time to react.

Acknowledgements

- xSigma contracts are based on others that have been hard tested with real money on mainnet. MasterChef, Curve, OpenZeppelin Delegator, Swerve.
- Pool – an OpenZeppelin Proxy ("Delegator") to Curve 3pool - Swerve used the same scheme successfully.
- Distributor – MasterChef.
- SIG token – SushiToken which itself uses modified Compound governance.