Modulus Protocol – White Paper

Revolutionizing Crypto Earnings: The Fairly Manipulated Randomness Finance Model Unveiled

Wayne Nguyen
wayne@modulus.fi
October 15, 2023

Introduction

1.1 Summary

The Modulus Protocol introduces Fairly Manipulated Randomness Finance Model (FMRFi), a transformative paradigm in decentralized finance (Defi), offering users the opportunity to earn significantly higher returns while keeping risk exposure controlled. Modulus Protocol and FMRFi are supposed to empower participants to actively engage in a rewarding venture, transforming staking into a dynamic endeavor. With the Chainlink Verified Random Function (VRF), the protocol selects 3 winners weekly based on deposit size and duration, ensuring an equitable opportunity for every participant to secure substantial rewards.

Modulus Protocol leverages its native token, $MODUL, as a means to enhance value for its holders. Locking $MODUL for a minimum of 3 months grants users Cheating Tickets, distributed in proportion to the lock amount and duration. These tickets offer users a strategic advantage in the protocol's pools, underlining the commitment to rewarding sustained participation.

This forward-looking approach challenges the conventional belief that higher rewards necessitate greater risks, presenting an innovative solution that harmonizes augmented returns with prudent risk management.

1.2 Scenario

As Defi gains momentum, it's imperative to recognize the underlying challenges that participants face within this rapidly evolving landscape. The Modulus Protocol stands as a beacon of innovation, aimed at addressing and resolving some of the fundamental problems that have lingered in the realm of decentralized finance. Let's delve into these issues, examine their implications, and explore how Modulus Protocol and FMRFi are uniquely positioned to provide solutions.

Limited Yield Potential: A prevalent problem in both traditional staking models and certain DeFi platforms is the limitation on yield potential. Investors often find themselves entrapped within fixed or minimal annual percentage yields (APY). This constriction stifles their ability to achieve significant returns, forcing them to explore higher risk strategies to attain better gains. This limitation poses a roadblock for individuals who aspire to grow their investments without subjecting themselves to disproportionately high risks. Imagine an investor participating in a DeFi staking pool where the annual returns are barely a few percentage points. Despite their commitment, the returns remain underwhelming. The reason behind this is that conventional yield models lack the adaptability required to optimize returns based on the prevailing market conditions and trends. This eventually make investors seeking substantial returns are left with limited options, leading to discontentment and the pursuit of riskier strategies to achieve their desired gains.

Lack of Long-term Engagement Incentives: Striking a balance between risk and reward is a challenge that Defi participants, and even traditional investors face. A plethora of Defi platforms offer either low-yield, low-risk options or high-yield, high-risk alternatives, leaving users without a middle ground to optimize their investment strategies. Limited availability of investment options that cater to varying risk appetites leads to an either-or scenario for investors. At the end, risk-averse individuals may miss out on potentially higher returns, while those open to risk may face significant losses.

Monotonous User Experience: Staking, Claiming, and Withdrawing – Those are boring actions that Web3 users have made repeatedly in years, indicating that Defi platforms often struggle to deliver an engaging and dynamic user experience. The repetitive nature of staking and yield farming processes can lead to monotony, reducing user interest and long-term engagement. The absence of innovative user engagement strategies and interactive features contributes to a lackluster user experience. Decreased user engagement, reduced participation, and diminished vibrancy within the Defi ecosystem is foreseeable.

1.3 Solutions by Modulus Protocol

The rapidly evolving landscape of DeFi is giving rise to innovative solutions that challenge established norms. As the demand for crypto-based investments escalates, the quest for higher returns accompanies it, leading to the emergence of novel paradigms. Traditional staking mechanisms have long provided returns with fluctuations in the range of 3% to 5% (APY). However, a transformative decentralized protocol, bearing the moniker of the Modulus Protocol and FMRFi, is poised to reshape these conventions and redefine the DeFi landscape.

At the heart of Modulus Protocol is FMRFi, a visionary concept that empowers users to earn substantially higher returns without commensurate increments in risk exposure. This introduces a paradigm shift that transforms conventional staking and liquidity farming into a dynamic and potentially lucrative venture. Central to this protocol are various tokens, including Lido Staked Ethereum (stETH) and other assets on all Ethereum Virtual Machine (EVM) chains, familiar to the stakers, which are elevated from the passive act of holding into a participatory and rewarding engagement.

In this Whitepaper, stETH would be taken as an example to describe Modulus. In stark contrast to conventional frameworks, where stETH holders contend with returns fluctuating within the range of 3% to 5% Annual Percentage Rate (APR), the Modulus Protocol disrupts this norm. Rather than passively holding stETH, participants can opt to deposit their tokens into a sophisticated smart contract deployed by Modulus. This strategic choice enables the contract to capture and accumulate the yield over the time. In traditional models, the yield is usually distributed proportionally to the participants. This leads to the aforementioned boredom, and this is where Modulus comes to bring about the excitements. Here, rather than sharing rewards across all participants, Modulus would only distribute the yield to 3 lucky users in which 50% would go to the first winner, 30% would go to the second winner, and the rest to the third one. To ensure the fairness, lucky users would be picked using VRF. Technically, Modulus's system would first summarize all of the pool's details in a 7-day epoch, including the amount of yield accumulated, the number of participants in the pool, the ticket amount of each user, and the ticket amount of all of the users. After that, Modulus's smart contracts would invoke VRF's smart contract to generate 3 random numbers which would then be matched to the users' ticket ID to come up with the lucky ones.

Beside bringing a feeling of expecting to the users, this selection process brings a unique dimension to the Modulus Protocol's structure. It goes beyond favoring a small, pre-defined group. Instead, it embraces inclusivity and fairness. Every participant who deposits into the protocol gains a chance to be selected, but the depth of engagement also matters. Those who deposit more and commit to longer staking durations increase their likelihood of being chosen. Consider the following example:

Imagine a scenario where users deposit into stETH pool. User A deposits a substantial amount of stETH and maintains the deposit for an extended period, amplifying their chances of selection. In contrast, User B deposits a smaller amount but holds the deposit for a shorter duration, resulting in fewer chances. This example indicates that FMRFi would bring benefits to all types of users. In the case of user A, he is manipulating his own possibility of winning leading to his high chance of winning. On the other hand, while user B's chance of winning is lower, he still stands a chance of winning exceptional rewards that he may even not be able to gain in years. This innovation aligns with the

Modulus Protocol's fundamental principle: maximizing returns without compromising risk tolerance. The chosen beneficiaries find themselves presented with not only a stroke of luck but also the assurance of substantial rewards.

One dark point in this model is that the participants may lose the yield that they may earn with traditional models. However, first, this loss is not significant which is estimated to be 0.008% - 0.013% daily. Secondly, this is supposed to be a valuable trade-off in which users may earn huge amount of profit that they may even not be able to earn in years with approximately 0 risks attached. Thirdly, Modulus's Tokenomics may help the users forget this. Here, in $MODUL's Initial Token Distribution, there is a proportion of 20% of the whole supply would be used to reward the community, helping the participants to, beside earning stable streams of yield like other traditional models, have huge chances of winning huge rewards.

In FMRFi, especially in Modulus's model, $MODUL plays an important role that would enhance the value proposition for its holders and for the protocol's participants, and an important role in Modulus's long-run existence. Here, by locking $MODUL for a minimum of 3 months, users who have deposited their tokens into Modulus's pools would receive Cheating Tickets on a weekly basis. The distribution of Cheating Tickets is proportional to the lock amount and duration, creating a direct correlation between commitment and rewards. These tickets can then be strategically allocated to Modulus Protocol's Pools, providing users with increased chances of winning, manipulating their own chances of winning. This innovative feature underscores the protocol's commitment to rewarding long-term engagement and participation. However, to keep the pools' attraction, the increased ticket amount would be limited to at most twice of the users' normal odds each Epoch.

In the initial phase of Modulus, the focus is on stETH on Ethereum Mainnet as the main pool of the protocol. This strategic decision enables us to offer diversified investment avenues, propelling the protocol's growth and Total Value Locked (TVL) to unprecedented heights. One interesting point of Modulus Protocol is that its Smart Contracts are designed to fit different yield models. This means that Modulus can be easily integrated into different types of investing, such as Liquidity Farming, Lending and Borrowing, etc., bringing excitements to broader number of Defi communities.

In an era defined by innovation, the Modulus Protocol stands as a testament to the power of ingenuity. Through a fusion of advanced technology, equitable distribution principles, and an unwavering grasp of human aspirations for financial growth, our protocol shapes a decentralized finance future that is inclusive, rewarding, and balanced.

To sum up, Modulus commits the three below key features:

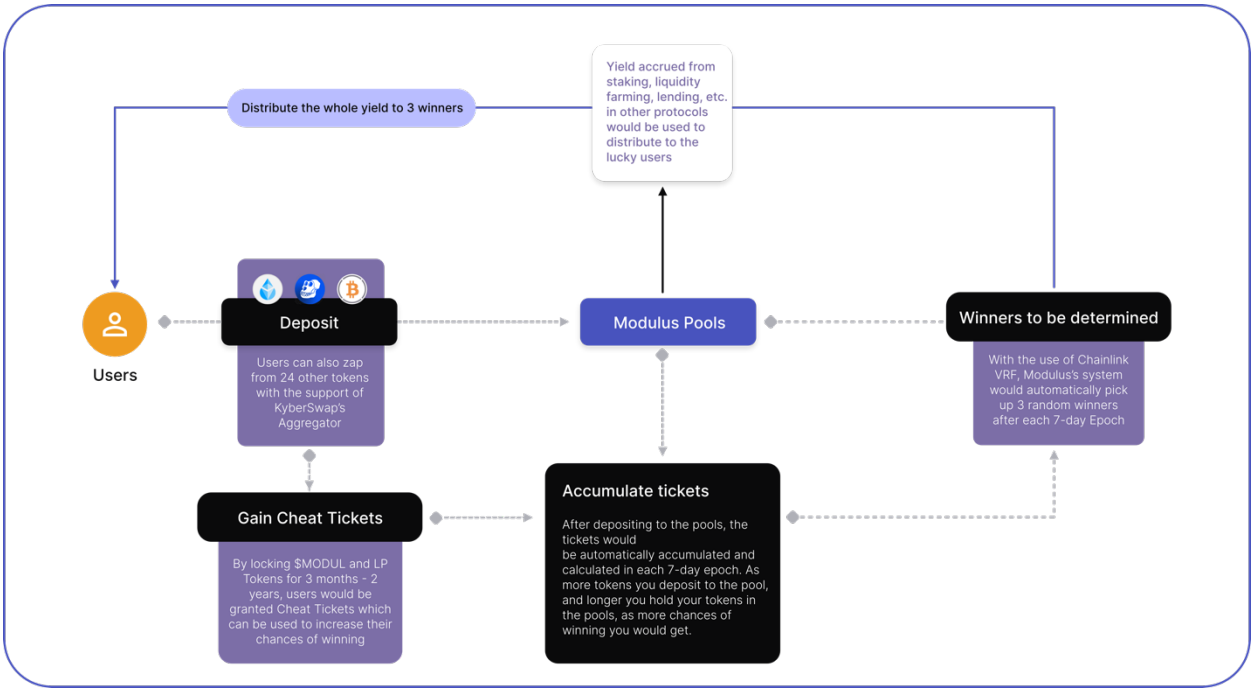
Skyrocketed Returns with Risk Controlled: Unlike traditional staking options that offer modest APRs, Modulus Protocol takes returns to new heights. With the potential to earn up to infinite APR, users can watch their investment flourish without taking on proportionally higher risks. Whether you're a cautious investor or seeking bolder gains, Modulus Protocol offers a dynamic yield model that adapts to your aspirations.

Fairness for all: Tired of seeing larger stakeholders reap all the rewards? Modulus Protocol breaks the mold by ensuring everyone has an equal shot at substantial earnings. Thanks to our innovative

use of VRF, every participant, regardless of their deposit size, stands a chance to be boomingly rewarded. For those depositing more and holding longer, they would have more chances of winning, and have a feeling of manipulating their own destinies. For those depositing less and keeping the tokens in the protocol shorter, they still have a huge potential of winning unbelievable rewards.

Engaging Excitement: Experience Defi like never before with Modulus Protocol's weekly selection process. With the use of VRF, the suspenseful winner-picking event adds an element of thrill and anticipation to your financial journey. It's not just about staking – it's about engaging with an ecosystem that keeps you on the edge of your seat. Get ready to be captivated, entertained, and rewarded in ways that traditional staking platforms cannot match.

Structures and Operations



2.1 How it works?

All pools operate according to the below steps:

Users deposit to pools: Users can choose their own desired pools to deposit tokens to. Each pool has its own required token. For example, to participate in stETH pool, users would be required to deposit stETH into the pool. With the integration of KyberSwap's Aggregator, Modulus Protocol support users to zap from 24 other common tokens into the pool. The deposited tokens would be used in different ways based on the strategy of the pool. In the case of stETH, as it's a rebase token, it would be kept in the pool's smart contract to accumulate the yield. In other cases, the tokens can be used to deposit to other protocols such as AAVE, APE Staking, etc. to gain the yield which would eventually be distributed to the lucky users.

Accumulating Tickets: In each Epoch, by depositing into pools, users would be automatically granted tickets which would then be used for the random lucky winner selection process. The tickets are determined by the users' deposit sizes and the time of holding the tokens in the pool. This indicates that if users deposit more tokens into the pools, and keep the tokens longer there, their winning chances would be improved. Please note that, thanks to our smart contracts' advances structures, the tickets would be automatically accumulated, and users will not have to do anything other than depositing into the pools to be eligible for winning the rewards.

Lock $MODUL or LP Tokens (Optional): Users can opt to purchase $MODUL and lock the token or LP Tokens to gain Cheat Tickets. The Cheat Tickets can then be distributed to the users' desired pools to increase the winning chances of the users. To keep the rewards attractive, the maximum additional tickets that users can get with Cheat Tickets is as twice as the tickets that the users get with pool tokens deposited.

Determining lucky users: At the end of each Epoch, Modulus would invoke Chainlink VRF to transparently get 3 random numbers. Those numbers would then be matched to users' ticket IDs to determine who the winners are. The 3 winners would get the rewards of 50%, 30%, and 20% respectively of the whole yield of the 7-day epoch.

Claiming rewards: After determining the lucky users, the winners would be announced via Modulus's Website, Discord, Twitter, etc. The winners can then claim the rewards immediately after winning the rewards or can claim them anytime.

2.2 Ticket amount

Ticket Amount is important in determining the lucky users. Let's take the below example to understand it further.

- Drake's userID stored in our smart contract is 1, and he got 500 tickets in Epoch 0
- Kanye's userID is 2, and he got 1000 tickets in Epoch 0
- The total amount of tickets in Epoch 0 is 115,000

Regarding userID, it would increase when there is a new user, and this will not affect the randomness and the chances of winning of each user. For example, Drake is the first one participating the protocol, his userID would be 1. Kanye is the second one and his userID would be 2.

With the above data retrieved from the Blockchain, our bot would consider Drake has ticketIDs ranging from [0 - 499] (500 tickets). The next user's ticketID would increment starting from the last one's ticketID, which means Kanye would have ticketIDs ranging from [500 - 1499] (1000 tickets).

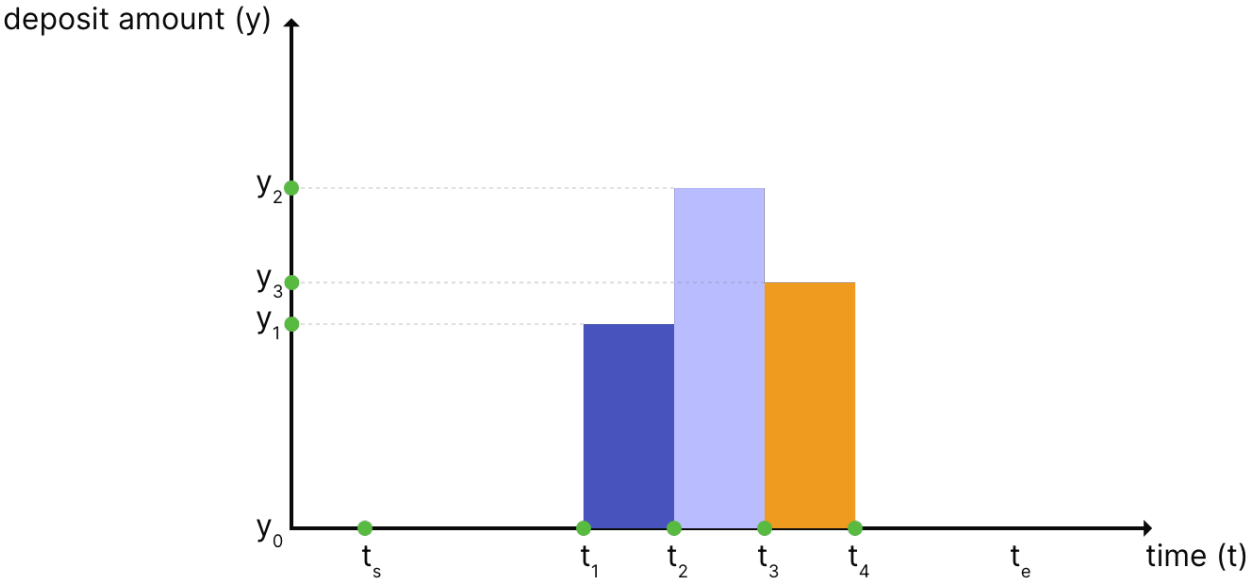
After arranging all the above steps, a request to Chainlink's VRF to get a random number would be made. Chainlink would then give us back a random number ranging from 0 to the max number of uint256.

For example, after sending a request to Chainlink, the service returns 9823472271002 as a random number. However, this number is too huge and is bigger than the total amount of tickets that the Epoch had. So, we would use Modulo to make sure that a user's ticketID would match the random number, which means the lucky user's ticketID would be equal to the remainder of the division of the random number, divided by the total number of tickets. So, it would be

$$9823472271002 \,\%\, 115000 = 1002$$

1002 is in Kanye's ticketID range; as such, Kanye is the lucky winner of Epoch 0.

The above example has explained how lucky users are chosen. Next, let's see how ticket amount is determined in each Epoch, and how it affects the winning possibility of each user.
Basically, users' winning possibilities are calculated based on the duration that the user has stayed in the pool in each 7-day Epoch, and the number of tokens deposited. Mathematically, we use integral to calculate the ticket amount users have in each Epoch.



$$t_s = \ starting\ point\ of\ an\ Epoch$$
$$t_e = \ ending\ point\ of\ an\ Epoch$$
$$t_n = \ updating\ point\ of\ the\ user\ (either\ deposit\ and\ withdraw)$$
$$y_n = \ balance\ of\ the\ user\ after\ depositing\ or\ withdrawing$$
$$y_0 = \ 0$$

$$ticket\ amount = \ [(t_1 - t_s) * \ y_0] + [(t_2 - t_1) * y_1] + \cdots + [(t_n - t_{(n-1)}) * \ y_{(n-1)}] + [(t_e - t_n) * \ y_n]$$

In the pools' smart contracts, every time a user deposits or withdraws, his ticket amount would be updated via the below function:

```
function _updateAccumulatedTicket(uint256 userIDnow, uint256 beforeUpdateBalance, uint256 latestUpdatedBlock, uint256 currentEpoch) internal
```

The variable accumulatedTicket[Epoch ID][User] would be increased by $[(t_n - t_{(n-1)}) * \ y_{(n-1)}]$ each time.This would be used to calculate the user's final ticket amount. In order to give the conveniences to the users making them do not have to do anything, our smart contracts would automatically calculate the amount of tickets that is not accumulated (As there are many cases users have no changes since the last updated time till the end of an Epoch), and then sum it up with the user's accumulated ticket to get the final ticket amount of the users.

Though the users' odds (Eg, user A has a winning chance of 1:500) does not say anything, it helps users to know what their winning rates are, and then know how to improve the rates. The following formula best describes how the winning possibility of a user is determined.

$$User's\ winning\ odds = user's\ ticket\ amount : total\ ticket\ amount\ of\ all\ users$$

Technology

3.1 Smart Contracts

Modulus is powered by smart contracts written in Solidity, and would initially be deployed on Ethereum Mainnet, including the below parts:

Deployment Factory: In order to help users to quickly and easily detect Modulus's Smart Contracts, all of the contracts would be deployed with the prefix 0x77777 and would be deployed via the Deployment Factory.

Router: The contract manages user deposits, withdrawals, and reward claims for different pools. Users can deposit tokens into supported pools, withdraw tokens, and claim rewards earned from participating in these pools. The contract also allows the addition and removal of supported pools by the controller role.

Role Registry: The contract is designed to manage roles and their associated addresses within a decentralized application. It allows for the initialization of key roles, including owner, controller, reward distributor, router, operator, VRF consumer, and reserve address. The contract offers functions to transfer ownership, set role addresses, and provides visibility into the current addresses associated with these roles while enforcing access control through a custom "onlyOwner" modifier.

Reward Distributor: This contract relies on Role Registry, VRF and pools for role management, pool operations, and randomness generation. The contract allows the owner and operator to initialize epochs, claim rewards, request randomness, and finalize epochs, ensuring fair and random reward distribution in the ecosystem. Please note that normal users have no access to this contract.

Reward Reserve: This contract is designed to manage the distribution of rewards. It utilizes a registry pattern, where the address of a registry contract is set during initialization and can be only changed by the owner. The contract allows authorized pools to transfer rewards (ERC-20 tokens) to specified recipients through the transferReward() function, ensuring that only valid pools can initiate these transfers.

Pool Contract: This is designed for managing users' deposits, withdrawals, and distributing rewards to lucky users. It allows users to deposit, and withdraw the tokens, claim rewards, tracks user deposit information, calculates rewards based on user deposits, and supports the creation and finalization of epochs for reward distribution. The contract can be configured with various parameters, such as reward allocation percentages and minimum deposit amounts. There are different types of pool contracts written; however, most of them are similar and the part interacting with other protocols is the only part that varies between them.

3.2 Security

Users' security is not just a priority to Modulus – it's our unwavering commitment and guiding principle. We understand that in the rapidly evolving landscape of decentralized finance, safeguarding user assets is paramount. That's why we go the extra mile to ensure that security is woven into every facet of our platform. From the moment users interact with Modulus Protocol, they can trust that their data, transactions, and investments are shielded by Modulus. We leave no stone unturned in our pursuit of airtight protection: rigorous audits, continuous monitoring, and proactive vulnerability detection are just a few elements of our comprehensive approach. As a team, we are dedicated to setting the gold standard for security in the blockchain realm, giving our users the peace of mind to explore, transact, and grow with confidence. Your security is not just a feature – it's our unshakable commitment to your financial wellbeing. Below are 3 important policies in developing the Protocol that our developers have aligned with, and would always align with to build a long-term success for the protocol:

Continuous Auditing and Improvement: To ensure the utmost protection for our users, we have established a rigorous policy of Continuous Auditing and Improvement. Our dedicated internal team remains vigilant, tirelessly reviewing the code of our smart contracts day and night, seeking out any potential vulnerabilities before they can manifest into risks. We understand that prevention is key, and as part of our proactive approach, we engage with a diverse range of external smart contract auditors. This collaborative effort empowers us to identify and address potential risks swiftly, creating a fortified environment where our users' assets are safeguarded with the highest level of scrutiny and care.

Different Points of View Mind: Modulus Protocol recognizes that ensuring the highest level of security requires a multifaceted approach. Our commitment to transparency and vigilance drives us to embrace a diversity of perspectives when it comes to auditing and optimizing our smart contracts. While our internal team is composed of skilled experts, we understand the potential for biases to inadvertently influence the auditing process. To counteract this, we actively seek external auditors who bring fresh eyes and diverse insights to the table. We firmly believe that a collaborative effort involving a wide range of perspectives is the key to uncovering potential vulnerabilities that might otherwise go unnoticed. Just as a puzzle becomes clearer when viewed from multiple angles, the thorough assessment of our smart contracts benefits immensely from the collective scrutiny of industry professionals. By actively engaging with external auditors and fostering an environment of open dialogue, we are dedicated to providing a security framework that is not only robust but also enriched by the collective wisdom of the blockchain community.

Decentralization in Smart Contract Development: Modulus Protocol places the utmost importance on safeguarding the integrity of our smart contracts through a steadfast commitment to decentralization. Drawing lessons from unfortunate incidents that have befallen the blockchain ecosystem, we have implemented a multi-faceted approach to fortify our security stance. To this end, multi-signature wallets are instrumental in ensuring that no single point of compromise could lead to a detrimental outcome. By distributing key decision-making responsibilities across multiple authorized parties, we eliminate the vulnerabilities associated with centralized control. Furthermore, we employ a strategy of diversification, employing distinct wallets to carry out distinct functions. This strategic compartmentalization is designed to mitigate the risks associated with potential key

leaks, as no single compromised key could lead to catastrophic consequences. Through these meticulous measures, Modulus Protocol demonstrates its resolute commitment to the principles of decentralization and security, fostering a safer environment for users and stakeholders alike.

Complying with the above policies, we have done an Audit with PeckShield on Oct 06, 2023. Via this audit, 2 information-severity and 1 medium-severity vulnerabilities have been discovered. All of those do not affect the protocol's funds or users' funds, and do not affect the protocol's operation.

The PeckShield audit report provides valuable insights and recommendations for enhancing the security of the Modulus Protocol. By addressing the identified issues swiftly and implementing the recommended improvements, Modulus demonstrates a commitment to the safety and trustworthiness of its smart contracts.

Peckshield Audit Report: https://github.com/modulusprotocol/audit