



Insure Your DeFi Journey

Security Protocol Whitepaper

Security protocol Team 2021

Table of Contents

- About this document.....
- 1 **Executive Summary**
- 2 **Introduction**.....
- 2.1 DeFi Landscape
- 2.2 Market Demand.....
- 2.3 Existing Challenges
- 2.4 Core Value Creations.....

- 3 **Solution Overview**
- 3.1 Business Model.....
- 3.2 Use Case
- 3.3 Key Components.....
- 3.4 Architecture Design
- 4 **Core Features and Designs**
- 4.1 Permissionless
- 4.2 Products.....
- 4.3 Capital Model.....
- 4.4 Pricing Model.....
- 4.5 Risk Management.....
- 4.6 Investment Management
- 4.7 Staking and SCR Mining
- 4.8 Claim Assessment.....
- 4.9 Governance.....
- 4.10 Cross-Chain Coverage
- 4.11 Ecosystem
- 5 **Token Economy**.....
- 6 **Transparency**
- 7 **Network Security**
- 8 **Legal and Compliance Framework**.....
- 9 **Roadmap and Future Development Plans**.....
- 10 **Conclusion**

About this document

This document and any other document in association aims to outline envisions of the business concept and platform design for the System Protocol project, a new decentralized insurance platform underpinned by BSC BlockChain technologies and DeFi philosophies. The business proposal set out in this document is based on the prospect of the evolving digital era we envisage, as well as certain assumptions and information currently available and deemed reliable to us, subject to possible updates from time to time. Due to the nascent nature of DeFi, the views stated in this document are representative of the business ideas of our team solely, and do not constitute any investment suggestion to any digital asset, or explanation of the policies or opinions of any government or authority. References to certain specific industry terms, company names, or platforms trademarks, are for illustrative purposes only, and do not imply any affiliation with, or endorsement of any of those parties.

1 Executive Summary

In this paper, we propose Security Protocol, a new decentralized insurance protocol, to empower the risk protection infrastructure for the DeFi community. Security protocol offers portfolio-based insurance products with optimized pricing models to substantially lower the cost; launches insurance investment functions with SCR mining programs to create sustainable returns for the participants; and provide coverage for cross-chain DeFi projects to benefit the whole ecosystem.

2 Introduction

2.1 DeFi Landscape

Decentralized Finance (DeFi) aims to offer financial services by leveraging the decentralized technologies, mainly public blockchain networks, in an open and transparent manner with universal accessibility. It has been at the forefront of

innovations in the blockchain and crypto currency space since 2019, and exploded in 2020 with various projects blossomed. The total value locked (TVL) in DeFi has boomed in the past few months, which, as of Nov. 2020, has surpassed US\$14.35B1 ,and the number of monthly active users has hit a new high of 300,000 in Sept. 2020.

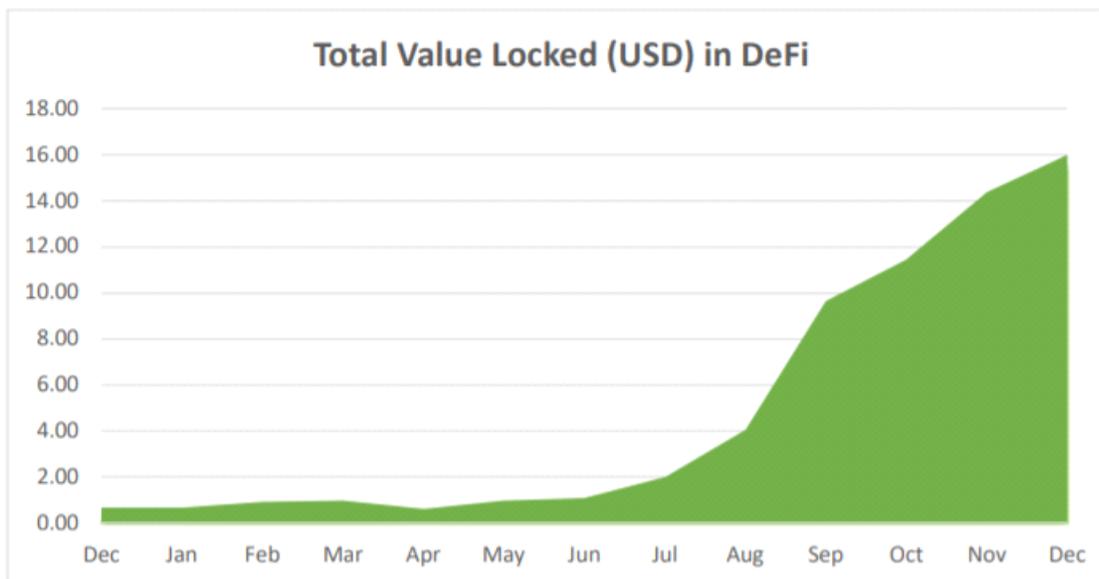


Figure 1 DeFi TVL Trend (from DeFi Pulse)

2.2 Market Demand

Since the inception of cryptocurrency, cyber security hack has been one the biggest challenges and threats to the industry. There are quite a few infamous and shocking attacks to the crypto space, such as the Mt. Gox hack back to 2011-2014 causing US\$460M loss, the NiceHash hack in 2017 causing US\$64M loss, the Bittrex hack in 2018 causing US\$18M loss and etc., which have been shaking the foundation of the crypto world.

With the advent of DeFi, the cyber security issues come along. There are 15 publicly

reported security hacks to the DeFi community since the 2nd half of 2019, including attacks to some well-known protocols, causing US\$113.26M loss in total

S/N	Time	Protocol	Loss (US\$M)	Exploits Description
1	22-Nov-2020	Pickle Finance	20.0	Code flaw in smart contract
2	14-Nov-2020	Value Protocol	6.0	Flash loan attacks
3	13-Nov-2020	Akropolis	2.0	Flash loan hacks
4	7-Nov-2020	Origin Protocol	7.0	Code flaw in smart contract
5	26-Oct-2020	Harvest	25.0	Flash loan attacks
6	14-Sep-2020	bZx	8.1	Code flaw in smart contract
7	6-Sep-2020	SYFI	0.25	Software bug
8	4-Aug-2020	Obyn	0.37	Double spend attack
9	28-Jun-2020	Balancer	0.50	Wrong price caused by oracle defect
10	19-Apr-2020	LendF.me	25.00	ERC777 token standard reentrancy attack
11	18-Apr-2020	imBTC Uniswap Pool	0.30	ERC777 token standard reentrancy attack
12	12-Mar-2020	Maker	9.00	Human manipulation
13	18-Feb-2020	bZx	0.64	Oracle manipulation (suspected)
14	15-Feb-2020	bZx	1.00	Flash loans and oracle manipulation
15	30-Jul-2019	Synthetix	8.1	Wrong price caused by oracle defect
Total Loss			113.26	

Table 1 Summary of DeFi Hacks

Needless to say, the cyber-attacks have been posing significant threats to the whole DeFi ecosystem fundamentally. Besides the technical approaches to resolve this problem, insurance, by its nature, has been another effective means to manage this risk. However, by taking a deeper look at the current DeFi landscape, insurance product still remain scarce especially for Binance smart chain.

2.3 Existing Challenges

We did extensive research on the existing insurance products, they are designed in different ideas and methods which can be categorized into 3 types with further comparisons listed in table below:

- Mutual insurance, such as the Nexus Mutual;

- Financial derivatives, such as the Oryn (convexity protocol); and
- Prediction market, such as the Augur.

Element	Mutual Insurance	Prediction Market	Financial Derivative
Product	Nexus Mutual	Augur	Oryn
Capital and Liquidity			
Common Capital Pool	Yes	No	No
Fully Collateralized	No	Yes	Yes (Nearly Always)
Liquidity	Customer to Pool	Two Sided Market	Two Sided Market
Flexibility			
New Products	Low	High	High
Risk Coverage	High	High	High
Claim Assessment	Voting	Voting	Not Required
Pricing			
Extreme Risk	Good	Not so good	Not so good
At the Money Risk	Not so good	Good	Good

Table 2 Existing Insurance Products Comparison

In spite of the development of existing DeFi insurance projects, we note that mutual is still the mainstream of DeFi insurance, however there are still a few common issues that need to be addressed.

(1) Limitations of Product Accessibility

There are some limitations on product accessibility for existing products, such as:

- High premium: especially for the protocols with less staked pool;
- KYC-based membership: which contradicts the free and open ethos of DeFi;
- Limited cover capacity: which often frustrates customers when they need to buy covers for their intending protocols;
- Lack of coverage for new protocols: which is often lagged behind the industry pace and unable to support the latest protocols;

- No cross-chain coverage: which limits the protection capability to DeFi protocols on other public chains;
- Lack of protection diversity: which is limited to cyber security protection only compared to the wide coverage of risk types in traditional insurance landscape;

(2) Lack of Underlying Risk Management

Risk management lies at the core of any insurance business, however current DeFi insurance products still have a lot of room to enhance their risk control capabilities, such as:

- Cyber security of the insurance protocol per se: what if the insurance platform itself is hacked?
- Concentration risk: the capital pool is often highly concentrated on a few major protocols, and the platform is solely relying on Binance Chain;
- Claim assessment: the existing claim assessment is handled in a gross manner with a Yes/No judgement only, without quantified evaluation of the loss;
- Operation / Credit / Market Risk evaluation: those risks are not well evaluated and taken into account for the platform design and operations.

(3) Capital Inefficiency

Capital efficiency constitutes the cornerstone for any insurance company, which benefits both the insurers and the insured in a systematic manner. However, low capital efficiency is another pain point for existing DeFi insurance products, such as:

- Low reserve utilization: the capital injected into the insurance platform is often not well managed, leading to the low utilization of the reserved fund which can be employed in a more delicate way;

- Unsustainable investment return: similar to traditional insurance business, customers are always expecting to gain sustainable investment return on the money they place into the insurance company.

We have seen the market demand for more insurance projects to enhance the risk management infrastructure of the DeFi ecosystem, as well as seeking for improvements to address the abovementioned challenges. Therefore, we would like to propose this solution, the Security protocol, with core value creations stated as below.

2.4 Core Value Creations

While we acknowledge and respect the leading role of Nexus Mutual as the pioneer of DeFi mutual insurance, we would like to build Security protocol as a mutual insurance protocol but with some distinctive value propositions. We do not consider ourselves as the competitor, but more of a healthy and necessary complementary role to the immense and expansive DeFi world.

(1) “0” Premium

With the portfolio-based product design as a fundamental approach of risk diversification, the premium for the insurance product will be reduced by its nature. Security protocol has also developed unique pricing models to optimize the cover cost leveraging on the expertise from insurance experts. Furthermore, the investment utilities will complement the cover cost to offer ultra-low premium, which is close to Zero at its best.

(2) Enriched Product Line

Unlike the single protocol based insurance coverage in Nexus Mutual, Security protocol will uniquely offer portfolio-based insurance product to enable coverage on a basket of DeFi protocols, which will create a diversified risk management tool for the DeFi investors. Despite the fact that Ethereum is the dominating public blockchain for DeFi protocols,

other public blockchain is also stepping in with booming DeFi projects. Security protocol will offer products to cover those non-Ethereum DeFi protocols as well to benefit the decentralized space as a whole.

Security protocol plans to expand the product accessibility to a wider audience by removing the KYC process. Anyone with a digital wallet will be able to connect with the platform and fairly use the services such as buying cover, staking asset, making claims and etc.

(3) Staking

Another distinctive feature for our token economy is our staking programs. The participants will be able to earn the Security protocol Token (SEC) by staking into the liquidity pool using BNB, DAI and/or other eligible tokens.

The mutual capitals injected through staking will be managed with rigorous risk control models to dynamically adjust the Solvency Capital Requirement accordingly.

(4) Sustainable Return

The low investment return has been a major challenge for Nexus Mutual since its capital return for the capital pool providers are sliced from the premiums, which is quite low compared to the benchmark yield on lending and borrowing platforms such as Compound and Aave. Such low return will in turn impede the capital injection into the capital pool, and worsen the issues such as high premium and limited capacity.

On Security protocol, customers will be able to gain returns in many ways, including:

- i) invest directly in other DeFi protocols per their risk appetite;
- ii) stake in the mutual pool to get Security protocol Token (SEC) as rewards.

We believe such design will benefit both the insured and insurers in a sustainable way.

(5) Further Improvements

Some of the processes will also be refined to better cater customer needs, such as:

- Handle claim assessment quantitatively instead of simple Accept or Reject;

- Provide extension, incremental or transfer capabilities to existing covers;
- Collaborate with other DeFi protocols to form an ecosystem to provide cross insurance, insurance syndication and etc. to benefit Security protocol customers;

3 Solution Overview

3.1 Business Model

As an insurance protocol, Security protocol will provide two function arms similar as the traditional insurance company, i.e., the insurance arm and investment arm. The free capital in the insurance capital pool can be placed into the investment pool to gain higher yield, while the insurance arm will provide protection to the investment activities. Meanwhile, the yield at the investment side will in turn complement the premium at the insurance side, and further reduce the cover cost for customers. These two parts will in such a synergetic manner to provide “0” premium insurance as well as considerable investment return, forming a sustainable business model.

3.2 Use Case

There are many use cases on the Security protocol , we will introduce three most typical cases for common Security protocol users and one platform level use case to further illustrate how Security protocol works.

(1) Investor

As an investor, Bob invests asset via investment portal by choosing the investment portfolio with different risk and return appetite. His investment will be covered by an almost “0” cost insurance and he will gain investment returns and SEC token as incentives

(2) Mary as an Insurer

As an insurer of the mutual, Mary stakes assets into the mutual insurance pool, gains SEC token as incentives according to the SCR mining and investment returns.

(3) Jack as an Insured

As an insurance customer, Jack accesses through the insurance portal to buy single or multiple insurance covers, get SEC tokens as incentives and request for claims when the policy is triggered.

(4) Synergy between the two Arms

Investors, insurers and insured will all benefit from the interactions between the investment and insurance arms at the platform level.

- The insurance arm provides coverages to the investment arm;
- The free capital in the insurance pool will be used for investment managed by the investment arm;
- The investment yield will be returned to the insurance side to incentivize the insurers and insureds.

3.3 Key Components

Based on the major use cases, the Security protocol will comprise of eight key components, including:

- Products: to provide enriched product line;
- Capital Provision: to inject liquidity into the mutual pool and investment vaults;
- SCR Mining: to manage the capital pool according to capital requirements and control the speed of liquidity mining;
- Investment: to generate investment yield for customers and further lower cover cost.
- Pricing Models: to design professional pricing methodologies to effectively lower the cover cost;

- Risk Management: to evaluate the risk of protocols on-boarded as well as manage the whole risk of the platform;
- Claim Assessment: to handle the claim requests from the cover buyers;
- Governance: to adopt DAO as the primary governance mechanism for product development, claim assessment, community proposals, token distribution etc.

Meanwhile, we'll also convene an Advisory Committee to handle the exceptions the contingency plan to safeguard the insurance business.

3.4 Architecture Design

The platform will consist of four layers, including:

- User Layer, to provide the user access functions for platform users such as cover buyers, investors, risk assessors and etc.;
- Operation Layer, to cover the various user or business operation scenarios interacting with core product functions;
- Products Layer, to build the core functions of the platform, such as product offering, liquidity pool, investment, pricing models, governance, etc.;
- Infrastructure Layer, to set up the interactions with Binance chain as a base, and maintain interoperability with external oracles and cross chain utilities.

4 Core Features and Designs

4.1 Permissionless

Unlike the Nexus Mutual platform where membership registration requires KYC process, which adds the complexity of centralized finance regulations, Security protocol platform will not require such KYC process, thus enable the platform reach to a wider audience. An Bep20 token, the Security protocol Token (SEC), will be issued as governance and utility token in Security protocol ecosystem.

4.2 Products

The Security protocol platform will provide covers on smart contract cyber threats at the start which is the most demanding in current DeFi space.

Unlike other single protocol based platform where capital pool and cover purchase is per protocol, Security protocol will adopt the portfolio-based design to pool all injected mutual funds into one pool and provide multiple protocol protection together. Basically, we plan to offer the covers in two approaches:

(1) User Defined Portfolios

When customers enter the Insurance Portal, they may choose one or multiple protocols as a portfolio to get a quotation and place the order, which is flexible and direct.

(2) Off-the-shelf Portfolios

To facilitate the customers, Security protocol will also provide some off-the-shelf product portfolios categorized by different criteria, such as:

- By protocol business type: a portfolio product to include the major protocols in Lending, or Decentralized Exchange (DEX), or Oracles and etc. so that customers can cover the risks of a business sector by one product;
- By protocol risk level: there will be an open risk assessment methodology to give a risk score for each protocol on-boarded, and a portfolio product that covers the same risk level protocols can be bought in one go.

At the start of platform launching, Security protocol will carefully select a list of protocols to be listed and offered. To on-board a new protocol subsequently, it will be mostly based on proposals from the community and subjected to community voting, in which the risk assessment methods as set out in section 4.5 will be employed to form a risk score for the protocol and be accounted into the pricing process.

Along the way, other types of risks such as asset volatility, flight delay, disaster and etc. will also be considered to enrich the product basket and enable a more comprehensive

coverage.

4.3 Capital Model

The business model of the insurance industry, including insurance and reinsurance, is about taking risks, mutualizing risks, managing risks while remaining solvent, and profitable, in which capital model defines the capital required to cover the risks associated with such purposes.

The capital model adopted by Security protocol is referred to the EIOPA's Solvency II, which is the prudential regime for insurance and reinsurance undertakings in the EU. It sets out requirements applicable to insurance and reinsurance companies with the aim to ensure the adequate protection of policyholders and beneficiaries.

At the core of the new regulatory framework Solvency II is an economic risk-based approach, which should enable the assessment of the "overall solvency" of insurance and reinsurance undertakings through quantitative and qualitative measures. Under Solvency II, the solvency requirements for the undertakings are determined on the basis of their risk profiles and on the way in which such risks are managed, therefore providing the right incentives for sound risk management practices and securing enhanced transparency.

There are different tiers of capital requirements under Solvency II, among which the Solvency Capital Requirement (SCR) and Minimum Capital Requirement (MCR) are the two key criteria. The SCR is the capital required to ensure that the insurance company will be able to meet its obligations over the next 12 months with a probability of at least 99.5%, where MCR represents the threshold to correspond to an 85% probability of adequacy over a 12 months and is bounded between 25% and 45% of the SCR. For supervisory purposes, the SCR and MCR can be regarded as "soft" and "hard" floors respectively.

Mathematically, SCR is made up of:

$$SCR = \text{Technical Provision} + \text{Additional Funds}$$

The first item is actually the discounted best estimate of all future cash flows, namely, the expected claim losses and other expense minus future premiums receivable. In our case, the discounted best estimate (DBE) for a portfolio will be equal to

$$DBE = \theta_1 \times SBC + \theta_2 \times EL$$

Then, the overall DBE can be formulated as follows, which is to cover the whole underwriting

$$DBE_{all} = \sqrt{\sum_{i,j} Corr(i,j) \times DBE_i \times DBE_j}$$

where $Corr(i,j)$ is correlations between each pair of Contracts.

The additional funds (AF) are reserved for the loss caused by "long tail" losses, which is calculated as follows,

$$AF_s = RF \times \sqrt{\sum_{i,j} Corr(i,j) \times CA_i \times CA_j}$$

where $RF \in (0, 1)$ is risk factor to scale the capital and CA_i is the Cover Amounts for individual portfolio i .

To operate with high standards of security, Security protocol will adopt SCR as the primary capital requirement which is more rigorous than existing platforms. The Free Capital excessive to the SCR in the capital pool will be used for investment in the investment arm of Security protocol to generate return for our participants, and reduce the cover cost as a whole.

4.4 Pricing Model

The insurance industry is largely an endeavor of hedging against uncertain future loss, in which the insured trade risks with the insurers by premiums via insurance contracts. Therefore, the pricing of insurance products lie at the core of any insurance business, and Security protocol has its unique offerings here as well.

Most pricing models in current blockchain-based insurance communities heavily rely on the value staked on individual protocols: the higher value staked for the specific protocol, the lower premium will be priced. This staking driven pricing structure fails to assess the real risk of each protocol and is very likely to significantly over-estimate the premium of those less staked protocols.

To substantially mitigate this issue, Security protocol will adopt new actuary-based pricing models to fairly assess the expected loss of insurance products, and thereby reduce the cost and enhance the capability.

The loss assessment is conducted on the portfolio level, which will consolidate portfolio level actuarial pricing and constituents' risk scores for each individual protocol involved in the portfolio.

4.5 Risk Management

Risk management is a key to ensure sustainable business model on Security protocol and guarantees the return on investment and protection. Security protocol introduces a three-step risk assessment approach for investment and protection protocols and bucket them into different risk categories.

(1) Expert Assessment

The Security Protocol Advisory Board will perform preliminary risk assessment on the new protocols at first with their expertise from relevant dimensions such as:

- Auditing reports of the protocol;
- Code analysis;

- Founding team qualifications;
- Operation track records;
- Relevance to existing hacked cases;
- etc.

Meanwhile, Security protocol will also work with the professional security auditing firms to seek for their support should there be extra complexity or challenges in due course.

After this, the Advisory Board will provide an assessment report and recommended risk score (1 to 5) as the reference for the community.

(2) Community Assessment

After the Advisory Board assessment, the protocol to be listed will also need to go through a community driven risk assessment which will be conducted by volunteered community members to further evaluate and get a risk score. The members who participate in this process will get SEC tokens as incentives.

With the above two steps, a final risk score will be given to the protocol.

(3) Continuous Update

Once the protocols is listed, we will employ the preparatory risk models to continuously evaluate risk level by collecting data and information of the given protocol, such as the staking changes, the claims to the protocol, correlation analysis to new security incidents, and etc. Such updates will be reflected into the existing risk model and provide up-to-date risk assessments.

Based on above risk assessment, protocols are bucked into different risk categories to construct investment or insurance staking pool with different return.

4.6 Investment Management

In the traditional insurance industry, the insurance company will use the funding from clients to invest in other financial products to generate returns for the clients. Similarly,

Security protocol will also carefully use the free capital secured from the SCR to invest in other DeFi products to gain investment return.

Security protocol will build an investment function similar as Yearn Finance, to design and implement the effective strategies. Customers can either directly invest via the Security protocol Investment Portal, or earn passive income with the free capital staked via the Insurance Portal. The built-in insurance capabilities will be able to seamlessly provide protections over the DeFi protocols invested, and the investment return will in turn complement the insurance customers, which creates a secure and sustainable investment cycle holistically.

Some potential investment plans that Security protocol investment will consider are as below:

- Yield farming on audited protocols and find the profitable investment paths;
- Stake the funds with lending platforms such as Compound to earn interests;
- Stake the funds in DEX such as Uniswap to earn the profits of liquidity providers;
- Other eligible investment strategies.

Any and all investment yields by right shall be returned to the customers, however a minor portion of it might be used to cover the transaction / operation cost, and other potential expenses incurred therein.

4.9 Governance

Security protocol will adopt the DAO governance mechanism commonly deployed in DeFi projects nowadays with SEC as the governance token for voting and incentive purposes. The principles for Security protocol governance are:

- Security of the capital that members deposit is at the highest priority. Use, movement, investment and/or any other key change to member capital shall be decided by the community;

- The day-to-day operations of the Security protocol platform shall not be impacted even without community involvement;
- Encourage maximum community participation in the key area changes such as business design, product listing/delisting, feature addition/removal, technology evolution, version releases and etc.
- In the event when community governance fails, there should be contingency procedures in place as the fall back plan to form a complete waterfall.

The governance framework will comprise of 2 approaches:

- Community Voting. Where there is any new proposals, the community can vote for or against the proposals until consensus is reached.
- Advisory Board, consists of InsurAce employees as well as 3rd-party independent advisors with technical, insurance, compliance and/or other required expertise. They work as the oversight committee to set certain rules, review the community proposal, as well as executing contingency plan when the community voting mechanism fails.

4.10 Cross-Chain Coverage

With the expansion of DeFi ecosystem, DeFi protocols built on other public blockchain such as TRON, EOS are also booming. Security protocol will firstly provide coverage to those non-Ethereum DeFi projects, providing coverage for the whole DeFi community. Along the way, we will also explore technical integrations with other public blockchains to grow with the whole ecosystem.

4.11 Ecosystem

Security protocol will collaborate with the DeFi projects that are insured to build an ecosystem where Security protocol clients or SEC holders will enjoy the benefits of those platforms.

For example, Security protocol users will be granted special incentives on insurance, lending,

DEX, and other protocols in collaboration with InsurAce.

5 Token Economy

The Security protocol platform will issue standard BEP20 token, SEC, as the governance and utility token to incentivize the participants in the ecosystem in a retroactively manner.

The SEC tokens can be used in below scenarios:

- Mining incentives for capital provisions to the insurance pool and investment products;
- Used in community governance scenarios such claim assessment, proposal voting and etc.;
- Community incentives;

6 Transparency

As a mutual based insurance platform, it bears in its nature to disclose the necessary information to participants, partners and other interested parties. Given the traceability and immutability of blockchain technology, all transaction data can be retrieved from the public distributed ledger, making the platform operations transparent. Meanwhile, we will disclose information and data on our website in a timely manner, including but not limited to:

- Transaction data of insurance products;
- Key metrics of the capital model, such as the SCR, SCR%, staking pool size, etc.;
- Parameters of the pricing models;
- Investment plans, executions and P/L;
- Platform operational cost and income;
- Claim process and executions;

- Community proposals and governance;
- Liquidity mining operation details;
- Token issuances, consumptions and distributions.

With these information publicized on the website, we aim to maintain a transparent and sustainable ecosystem where the platform can provide insurance covers to the whole crypto space. In the event when any inaccuracy or misinformation occurs, the InsurAce platform will respond timely to ensure the transparency of the whole community.

7 Network Security

The DeFi applications have been constantly exposed to cyber security risks which is what Security protocol intends to resolve via fine designed insurance products. As a fundamental risk management platform for the whole DeFi ecosystem, the security for Security protocol platform per se will be more critical than any other applications. To build a highly secure and resilient protocol, we will adopt the best practices in the industry, such as:

(1) Smart contract audits

We will invite 3rd party independent audit company to audit the smart contracts of InsurAce, to detect, identify and eliminate the potential contract vulnerabilities through rigorous code review, testing and white-hat hacking prior to the protocol launch. The audit reports will be released to the public.

(2) Deploy up-to-date security solutions

There are security solutions to monitor the health status of the network, on-chain activities, oracle dependencies, admin key details, etc., which will be adopted by Security protocol to surveil and enhance the platform security.

(3) Develop effective security incident response process

With the implementations of the above security controls, it is equally important to establish a process on how to properly respond to cyber security incidents. In the event when a security breach occurs, the Security protocol security team will respond timely with contingency plans, such as:

- Suspend or terminate partial or all functions of smart contracts;
- Add a pending session to some suspicious and large transactions;
- Revert suspicious transactions and trace back the root cause;

Overall, it is never overstated to enhance the platform security capabilities. With

Security protocol as a secure and resilient insurance protocol, the whole DeFi community will also be benefited in the long run.

8 Legal and Compliance Framework

Given the decentralized nature and nascent status quo of DeFi, the operators and/or participants of DeFi network may be exposed to legal and regulatory uncertainties as the existing statutory and compliance interpretations may not be up-to-date to address the emerging challenges. Nevertheless, Security protocol will carefully examine the existing applicable laws and regulations as well as stay tuned to latest updates to ensure full compliance with relevant legal and compliance jurisdictions.

9 Roadmap and Future Development Plans

We foresee that the development of Security protocol platform is a systematic project that requires persistent efforts and continuous improvements, which will be rolled out according to plans below for the 1st year.

Q2 2021

- Platform design and prototype protocol development.
- Community building.
- Private token sales.

Q3 2021

- Launch of Security protocol v1.0, including the portfolio based insurance products, capital pools, staking, investment portal, claim assessment and governance.
- Launch of Security protocol v2, to include the cross-chain DeFi protocol covers, enhancement to investment planning and implementations, continuous optimization of pricing models.
- Explore collaborations with other DeFi protocols.

Q4 2021

- Launch of Security protocol v3, to include insurance coverage marketplace, continuous enhancements to existing products and models, more collaborations with other DeFi protocols in the ecosystem

Q1 2022

- Diversify the product line to cover more risk types, such as oracle malfunction, asset volatility, flight delay, disaster and etc.
- Explore cross-chain technical integrations with other public BlockChains.
- Continuous enhancements to platform operations and expansion of market shares.

10 Conclusion

With the above designs and value propositions, we are committed to build the

Security protocol platform as an infrastructure for the whole DeFi community, and provide easy access, cost efficient, as well as fine governed insurance service to the millions of users in the digital era.