DEGIS Whitepaper

January 2022 @ v2.0.4

Abstract

The protection industry is enormous and plays an essential role in the financial market. However, there is cumbersome paperwork and claim procedures in the traditional way, which is unfriendly for users. However, with the increasing development of blockchain technology, things can become more efficient and secure under smart contract settings. A combination of high-advanced tech and time-honored protection products gives birth to DEGIS, our integrated decentralized protection platform.

1 Introduction

Protection, as the fundamental part of the financial market, has a considerable market volume. Related products such as delay protection, accident protection have been shown as effective in hedging various risks. Nevertheless, in the traditional market, companies need to hire sales associates to investigate personal information about customers before offering protection products. Also, there are rather complex paperwork and cumbersome claim procedures, limiting protection application scenarios.

With DeFi infrastructure, smart contracts will play sales associates' roles based on their immutable and forced automatic execution characteristics. We are thinking if there will be a platform where anyone can put their money to behave like a protection provider to help cover others' risks without complicated verification and settlement procedures.

In this paper, we present DEGIS, a novel Integrated Decentralized protection platform that entitles both liquidity providers and insureds to more flexible risk covering options with lower costs and higher returns. Technical advantages of blockchain and the big data analysis model benefit each participant engaged in DEGIS. Besides, DEGIS offers several significant features:

- Multiple coverages of on-chain and off-chain products.
- Concentraded pool to aggregate capital and liquidity.
- Secondary market to promote circulation.
- NFT attributes and lottery mechanism.

We think that in the future there will be four types of protection in the market: Token Model, NFT Model, Meta Model and DAO Model. These four kinds of protection have their own advantages and disadvantages and correspond to different usage scenarios. Through the interpretation, analysis and practice of these four types of protection, DEGIS hopes to be the pioneer of the decentralized protection.

2 Token Model

Token model protection is to tokenize homogenized events, then the protection contracts of events can be traded in the market freely. Homogenized events mean that the probability of the occurrence of the events has no relation with the identities of the parties to the contract, but is only related to objective external conditions.

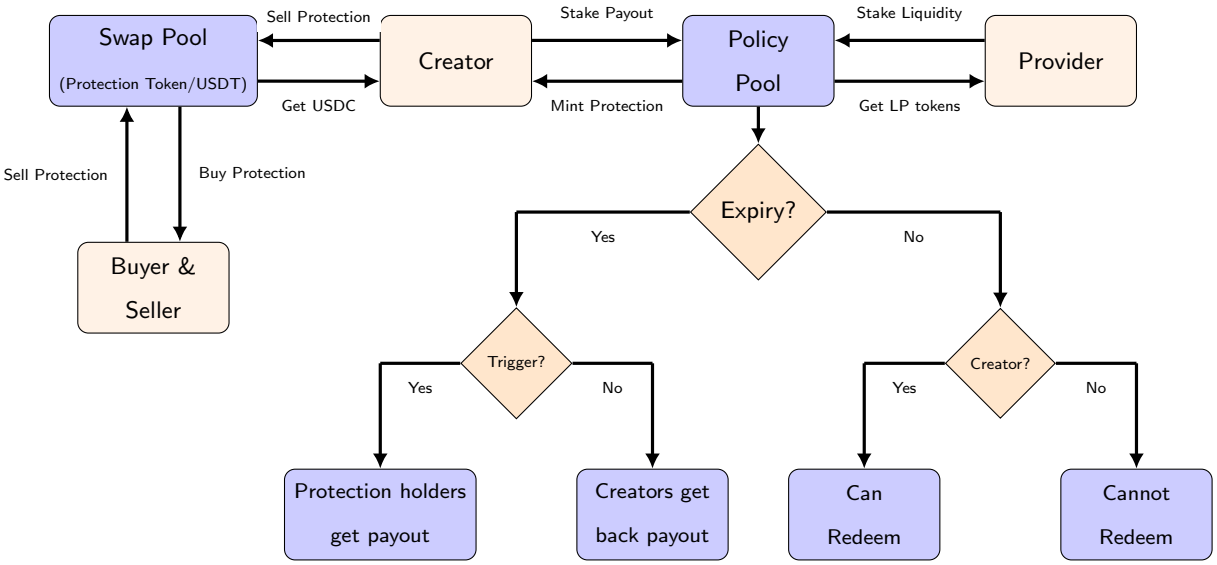

Figure 2.1: Workflow of the protection token system

2.1 Creation and Destruction of Protection Token

To mint a protection token for a certain event, one needs to make a full mortgage, which means staking the maximum potential payout to mint one protection token. The potential payout is staked in the policy pool. The minted protection tokens are fungible tokens and can be exchanged and transferred.

The staked potential payout in the policy pool is controlled by smart contracts. If the certain event happens at the expiry date,then the protection token holders can use their tokens to claim the payout. If the certain event does not happen at the expiry date, the staked money will be sent back to creators automatically.

Before the expiry date, creators can redeem their staked money by burning the protection tokens. The maximum total amount of redeeming is the total amount of protection tokens that the creators have ever minted.

2.2 Transaction of Protection Token

Since protection tokens are fungible tokens, we use AMM swap pools to trade protection tokens with other tokens. The swap mechanism is same as Uniswap V2. When someone wants to swap tokens in the pool, the product of the amount of tokens on two sides remains unchanged [1]. The transaction fee will be charged when the trader putting the tokens in the one side of the swap

pool, which is 2 % at EDGIS platform currently. Transaction fee will be used to reward liquidity providers. DEGIS will be the first one to provide liquidity for both sides based on our pricing model, then the pool will star running and the price will be decided by the market.

Creators can sell their protection tokens and earn profits. If the certain event according to the protection policy does not happen at the expiry date, creators can get back their staked money and these profits will be the final earnings. If the event does happen, they will lose their originally staked money. Some cautious creators may repurchase the protection tokens after selling, and redeem their staked money to avoid loss of principal.

Creators can also choose to be liquidity providers by putting the paired tokens in both side of the swap pool. In this way, they can earn low-risk transaction fees. The risk for liquidity providers is that if the price of the protection tokens fluctuates a lot, the impermanence loss may be larger than earned transaction fees. To avoid possible large impermanence loss near the expiry date, DEGIS will close the swap pool three days before the expiry date. Traders can not swap in the pool after closing, but liquidity provides can withdraw their liquidity.

2.3 An Example of Token Model — Token Price Protection

The crypto market has a large variation, and investors may suffer a huge loss within a short period. To help investors hedge the extra risk, DEGIS issues a new kind of protections upon token price fluctuation. There are two kinds of token price protection.

- *Cover Price Decreasing*

  The policy event is that when the price of a certain token falls below the strike.

- *Cover Price Increasing*

  The policy event is that when the price of a certain token rises above the strike.

There is a set of naming methods for protection tokens. For example, AVAX60L2202 means that this is a protection token for AVAX and can get payout if it is lower than $ 60 at the first day of February 2022. Protection tokens can star to be minted two months before the expiry date.

3 NFT Model

We set a public protection pool here on DEGIS, where liquidity providers can enter it acting as protection providers. Each protection would be activated by the platform and backed by the liquidity pool. This is very convenient for users with different needs and also helps concentrate capital and liquidity. Through big data analysis, we get rather precise prediction on expected payoff, which supports us to offer low and competitive price in protection market. On the other hand, the protection status is automatically updated through decentralized oracles, i.e., trustworthy third-party off-chain data service providers. The payoff will be cleared immediately once the protection is due. Comparing to the salesmen, smart contracts can reduce the manual cost and dramatically optimizes the user experience.

At any stage, our protection product will be packaged as NFT(Non-fungible token), with users' basic information on it. Once submit the protection order, the corresponding NFT will be minted and sent to the user's wallet directly. On the one hand, such non-fungible tokens have the connotation of protection service with certain intrinsic values. On the other, the NFT will not be burnt if backing protection does not get expired, users can keep it for collection and would be able to exchange discounts for other DEGIS designs in the future.

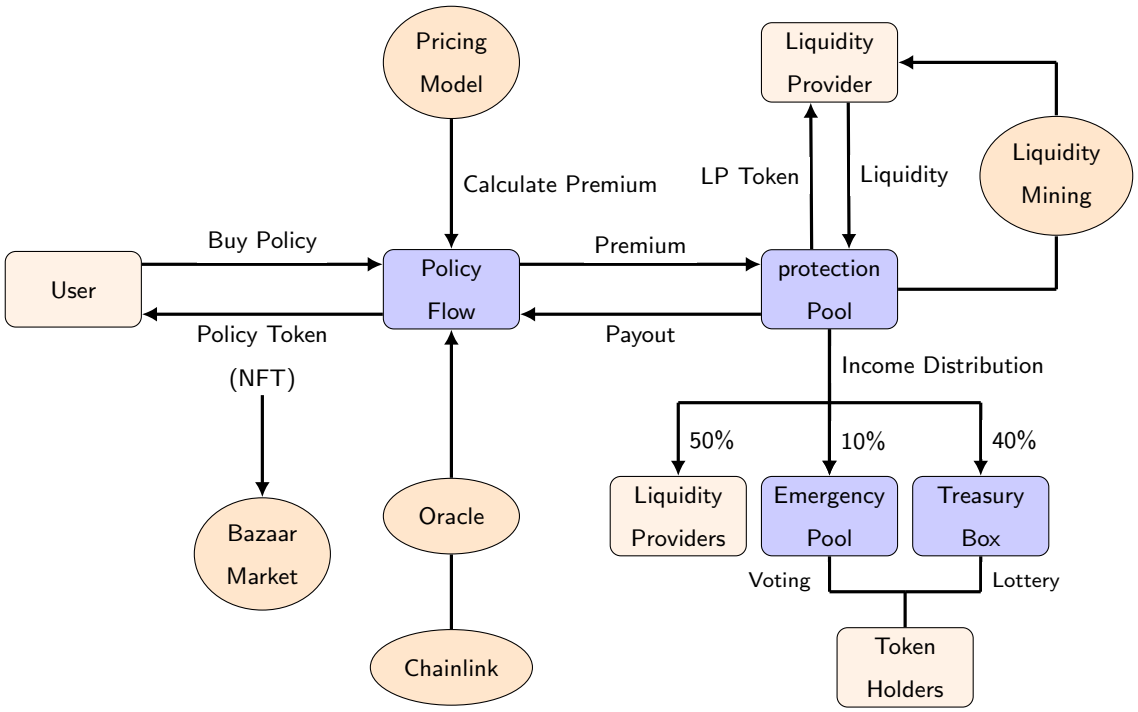

Figure 3.1: Workflow of the DEGIS platform

3.1 Provide Liquidity in the Protection Pool

3.1.1 Why Provide Liquidity on DEGIS

- Easy to enter, easy to earn.
- Permissionless to enter and exit.
- Stable premium income based on statistics.
- Additional token incentives.

3.1.2 How to Provide

As an liquidity provider, or to say, protection provider on DEGIS, you can get quick, upfront, and stable premiums from buyers through staking your money into the protection pool, then DEGIS platform will publish and sell protection policies for you. There is no minimum entry requirement, and you are free to exit at any time to withdraw all your liquidity. Profit/Loss will be settled at the time of withdrawal, which is proportional to the staking time and amount.

3.1.3 Risks and Benefits

Pooled liquidity is designed to reduce risks for individual liquidity providers. Big data analysis and advanced machine learning models help ensure stable income. In the appendix section, we provide some numerical simulation results for reference.

3.2 Buy Protection

3.2.1 Why Buy Protection on DEGIS

- Fair, transparent and automated.
- No central controller and disputing about policies.
- Simple operation and instant settlement.
- Rational price and significant payoff.

3.2.2 How to buy

Find NFT Model protection on DEGIS from the website (DEGIS.io), choose the type of protection product you'd like, and finally confirm with just one simple click! The protection NFT will show up in your wallet and the payoff will be directly sent to your address if protection conditions get met in the future. No other actions are required.

3.2.3 Risks and Benefits

Users should be well aware of the risks of protection products before buying them, and we would offer a relatively low price and high payoff to attract insureds in need.

3.3 Concentrated Liquidity

Different kinds of protection products will be backed by one same liquidity pool on DEGIS. Liquidity providers enter this pool to provide protection services and earn premiums.

3.4 Examples of NFT Model

DEGIS self-developed our first NFT Model protection — flight delay protection. You can see the detailed mechanism and simulation in the appendix. We are also developing impermanent loss protection and smart contract protection now based on our smart protection engine.

4 Meta Model

4.1 Aggregator

On-chain protection products including NFT Model protection and Token Model Protection can be traded in Meta Market which is an aggregator. Not only products from Degis, on-chain

protection protocols from other platforms can be called in Meta Market. Through Meta Market, in addition to helping users achieve simple functions such as one-stop order placement and price comparison, it can also perform advanced functions such as AI protection portfolio.

4.2 Customized Protection Contract

Nowadays, all protection contracts are fully developed by institutions. Users can not customize their own needed protection but can only accept institution-prepared contracts. DEGIS Meta Protection will empower users to maker their own smart contracts to generate customized protection. Users can easily do so by setting some simple variables including payout conditions, value setting, execution schedule etc. Then they can sell the protection or request an order in Meta Market.

5 DAO Model

DEGIS will provide users an easy way to form a protection mutual DAO which is backed by smart contracts. DAO members can jointly set the DAO entrance threshold and the regular membership fees. They can also formulate DAO's own payout rules and verification method.

6 Ecosystem

6.1 Tokenomics

DEG is the protocol token of DEGIS and its total supply is 100 million. Detailed distribution proportion is designed as follows:

- Purchase Incentives: 35%
  35 million DEG in total. To incentivize buyers to consume on Deigs platform. Release according to users' participation.
- Liquidity Rewards: 15%
  15 million DEG in total. To incentivize liquidity provides of all pools on Degis platform. Release according to users' participation.
- Team: 12%
  12 million DEG in total. Locked for 15 months once DEGIS launched on mainnet and then released quarterly in 15 months.
- Growth Fund: 7%
  7 million DEG in total. Mainly used for airdrop, marketing, DEX liquidity providing and business network. 1.5 million DEG are released at TGE. 5.5 million DEG are released quarterly in 24 months.
- Advisory: 3%
  Same locking mechanism with the team.

- Angel Round: 5%
  Total release in Core Round is 5 million DEG. Locked for 12 months once DEGIS launched on mainnet and then released quarterly in 12 months.

- Seed Round: 12%
  Total release in Seed Round is 12 million DEG. 10% of which are released at TGE, and 90% locked for 12 months once DEGIS launched on mainnet and then released quarterly in 12 months.

- Strategic Round: 4%
  Total release in Strategic Round is 4 million DEG. 12.5% of which are released at TGE, and 87.5% locked for 12 months once DEGIS launched on mainnet and then released quarterly in 12 months.

- Public Sale: 2%
  Total release in Public Sale is 2 million DEG. 100% released at TGE.

- Reserves: 5%
  5 million DEG in total. Used for emergency events(decided by the community).

6.2 Treasury Box

DEG holders can stake DEG to participant in Treasury Box. Users can mint one ticket which in an NFT after staking 10 DEG. Every week, there will be a random four-digit number generated by Chainlink which has 10,000 possibilities. Each ticket lets the user guess a number before the draw. After drawing, tickets which only guess the last digit right will share 20% of Treasury Box pool together. Tickets which guess the last two, last three and all four digits right will also respectively share 20% of Treasury Box pool. The remaining 20% will be left to the next term. One ticket can only get the reward for guessing the maximum number of digits.

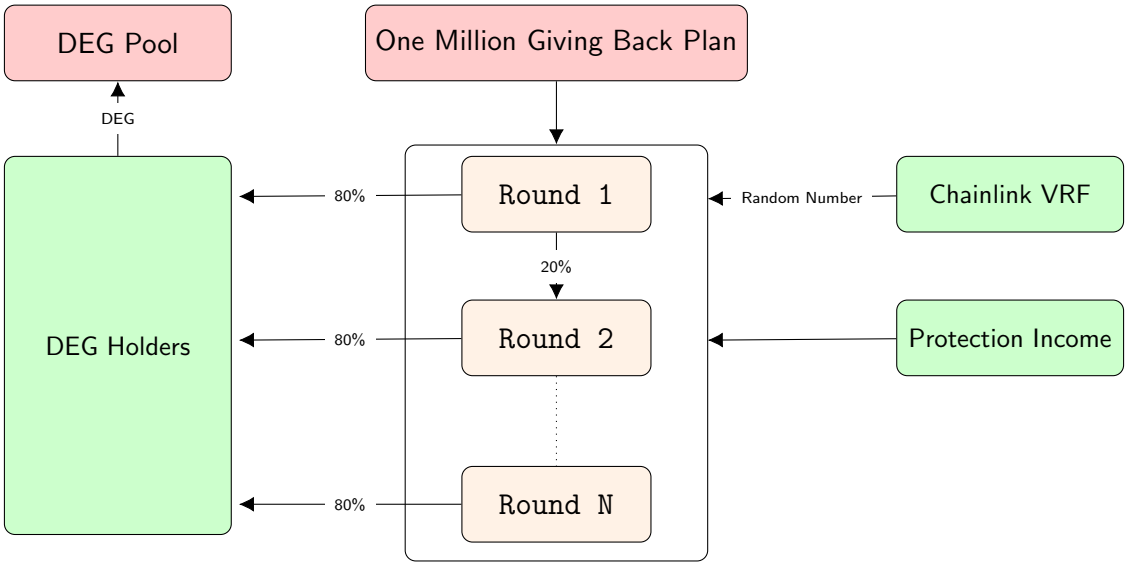

Figure 6.1: Recurrent lossless lottery game for DEGIS holders

When sharing Treasury Box between winning tickets, there will be different weights due to different initial staking time, which is a gradually decreasing function over time. For a ticket mined in the i^{th} term, the weight is

$$W_i = \frac{i+24}{i+12}$$

The guessing number of a ticket can not be changed once minted. If one uses the ticket to redeem DEG, the weight rewards will disappear and new weight will be calculated at the newly minting time.

The rewards in Treasury Box pool come from three parts. The mainly part is the protection income. Currently, 40% of the income of NFT Model and 1% of the money staked by creators in Token Model will be put in Treasury Box. The second part comes from One Million Giving Back Plan. In the next 2 years, DEGIS will ensure that at least $ 10,000 is distributed every week. The third part comes from the 20% left from the last term Treasury.

6.3 Purchase Incentive

In order to change the unreasonable status quo that many protocols have a large TVL but a small transaction volume, DEGIS brings out the unique purchase incentive mechanism. Users can get buyer tokens which are fungible tokens when they consume on DEGIS platform and the amount is equal to the USD they consume. Users can deposit their buyer tokens in the incentive pool. The pool will burn the deposited buyer tokens every 24 hours and reward DEG to buyers according to their deposit share. Users can withdrawal their buyer tokens freely before the daily burn. By applying this unique mechanism, we hope to build a more efficient and cyclical ecosystem.

6.4 Farming

DEG will be distributed to LP pools. LP pools include Naughty Price AMM pools and Miserable Flight liquidity pool. LP will share the DEG according to their LP token proportion in each pool.

6.5 Staking

6.5.1 Stake DEG

DEG will be rewarded to stakers who stake their DEG. Holders can set lock-up time to increase the allocation weight. The original weight for flexible staking is 1×, and the weight increases linearly to 2× when the lock-up time increases to 12 months. The rewarded DEG consist of two parts. One comes from the liquidity rewards planned by DEGIS team and the community. Another comes from the redistributed platform fees, which are charged 2% of the deposit amount at the staking time.

6.5.2 Stake DEG and DEX LP token

DEG will be rewarded to stakers who stake both DEG and DEG LP token of DEG pairs. The rewards calculated rule is the same to staking DEG. DEGIS will also set joint mining plan with DEC.

6.6 Governance

After the ecosystem runs smoothly, the decision-making power of mining rewards and purchase incentive will be given back to the community. Also, some future product development and major decisions will also be decided by the community. As DeFi industry grows stronger and soundness, we will continue to empower DEG.

7 Roadmap

Q3 2021

- Feasibility Research
- Data Analysis
- Protection Product Development

Q4 2021

- Smart Contract Development
- Website Release
- Social Media Release
- Community Building
- Testnet Phase 1

Q1 2022

- Auditing
- Testnet Phase 2
- Mainnet Launch
- IDO & TGE
- DEX & CEX Listing
- Partnership with Avalanche Eco projects

Q2 2022

- Avalanche Major Tokens Protection
- Launch Impermanent Loss Protection

Q3 2022

- Launch Smart Contract Protection
- Metaverse & GameFi add-ins

Q4 2022

- Initial Launch of Meta Market
- Community Governance

Q1-Q2 2022

- All-in-one Protection Aggregation
- Community Designed Products

Q3 2022

- DAO Model Protection

8 Appendix

8.1 Flight Delay Insurance Mechanism

8.1.1 Payout

Unlike traditional protection, which sets a fixed payout, DEGIS provides users with a continuous and increasing payout when delay time does exceed the threshold. Currently, the threshold is fixed at 30 (minutes), while users may set their preferred one in the short future. Detailed payout policy is stated in the following, where *threshold* as 30, t is the delay time in minutes and currency unit in USD.

$$Payout = \begin{cases} 0 & t < threshold \\ \frac{1}{480} \cdot t^2 & threshold \leq t < 240 \\ 120 & t \geq 240 \end{cases} \tag{8.1}$$

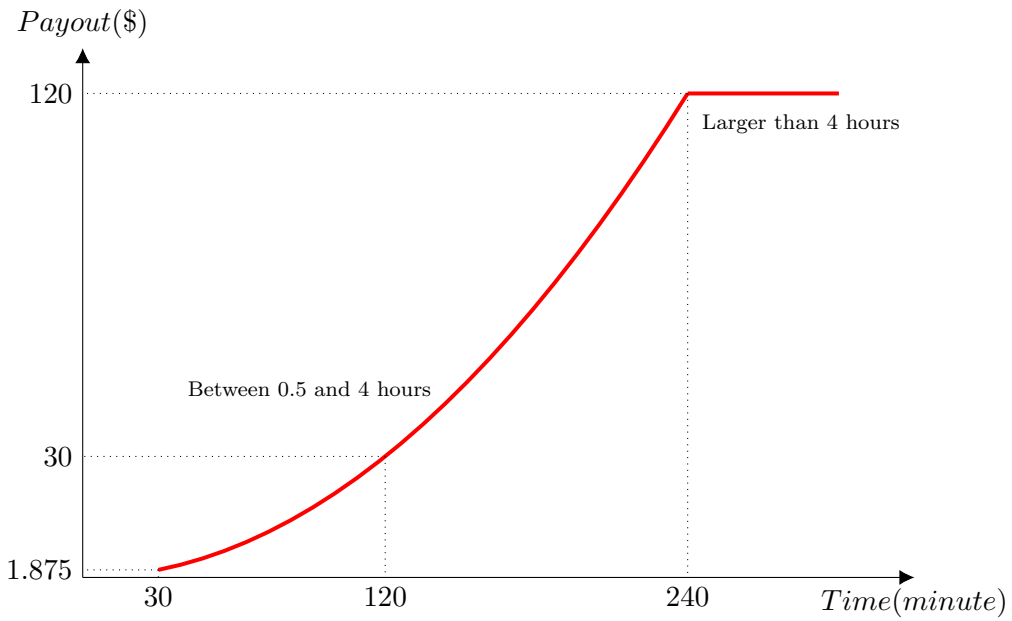

Figure 8.1: Function graph of payout amount and delay time

8.1.2 Pricing

DEGIS uses self-developed machine learning models to predict the expected payout of each flight, based on departure time, weather, airlines, airports, distances, associated flights, and many other features. Basic price will be the maximum between the predicted payout and 4.2 dollars. Which means, different flights may have different basic prices, but the majority of them will be 4.2 dollars.

We first divide the delay time into several intervals, leading to an ordered classification problem, and train gradient boosted regression trees with a squared loss penalty [2] $H'(\mathbf{x}_i) = \sum_{t=1}^{T} h_t(\mathbf{x}_i)$, where each function $h_t(\cdot)$ is a limited-depth CART tree. We then apply the mapping $\mathbf{x}_i \to \phi(\mathbf{x}_i)$ to all inputs, where $\phi(\mathbf{x}_i) = [h_1(\mathbf{x}_i), \ldots, h_T(\mathbf{x}_i)]^\top$, and refer these CART trees as *weak learners*. To solve our final prediction problem, we learn the weighted-vector β by minimizing a convex empirical risk function $\ell\left(\phi(\mathbf{x}_i)^\top \boldsymbol{\beta}, y_i\right)$ with l_1 regularization, $|\boldsymbol{\beta}|$. In addition, we incorporate a cost term $c(\boldsymbol{\beta})$, which we derive in the following statement, to restrict test-time cost. The combined test-time cost loss function is

$$\mathcal{L}(\boldsymbol{\beta}) = \underbrace{\sum_i \ell\left(\phi(\mathbf{x}_i)^\Gamma \boldsymbol{p}, y_i\right) + \rho\,|\beta|}_{\text{regularized risk}} + \underbrace{\lambda\, c(\beta)}_{\text{test-cost}}$$

There are two factors that contribute to the test-time cost of each classifier: the weak learner evaluation cost of all active $h_t(\cdot)$ (with $|\beta_t| > 0$) and the feature extraction cost for all features used in these weak learners. Define an auxiliary matrix $\mathbf{F} \in \{0,1\}^{d \times T}$ with $F_{\alpha t} = 1$ if and only if the weak learner h_t uses feature f_α. Let $e_t > 0$ be the cost to evaluate a $h_t(\cdot)$, and c_α be the cost to extract feature f_α. With this notation, we can formulate the total test-time cost for an

instance precisely as

$$c(\boldsymbol{\beta}) = \underbrace{\sum_t e_t \left\|\beta_t\right\|_0}_{\text{evaluation cost}} + \underbrace{\sum_\alpha c_\alpha \left\|\sum_t \left|F_{\alpha t}\beta_t\right|\right\|_0}_{\text{feature extraction cost}}$$

To take protection risks into account, we define $\tau = \mathbb{E}\left(\frac{L}{e}\right)$ where L is the loss and e the period for which the protection is valid(exposure). Assume that the size of the claims is independent of the claim frequency and orders' arrival (denoted as $A_t, a\ Poission\ Process$), we make follwoing expansion:

$$\tau = \mathbb{E}\left(\frac{L}{e} \mid A_t\right) = \mathbb{E}\left(\frac{L}{N} \mid N > 0\ , A_t\right) \times \mathbb{E}\left(\frac{N}{e} \mid A_t\right) := \mathbb{E}\left(S\right) \times \mathbb{E}\left(F\right)$$

where N is the number of claims, S the severity, or size of the claim and F the claim frequency(conditioned on agent behaviors).

Combination of all these to obtain our actual optimization problem (8.2)

$$\underset{\beta}{\operatorname{argmin}} \quad \underbrace{\sum_t \mathbb{E}\left(S|A_t,\beta\right) \times \mathbb{E}(F|A_t,\beta) + \rho\ |\beta_{\mathbf{t}}|_0}_{\text{regularized risk}} + \underbrace{\sum_t e_t\,|\beta_t|_0 + \sum_\alpha c_\alpha \sum_t |F_{\alpha t}\beta_t|_0}_{\text{test-cost}} \tag{8.2}$$

8.1.3 Prohibit Inside Trading

A total of 500 protections are available for sale on each flight episode, and in order to combat insider traders and malicious attackers, also protect the interests of ordinary consumers. Meanwhile, we have designed a price floating system with three rules:

- For a certain flight, the price increases 2% for every protection purchased(except for the first 20).
- For a certain flight on a certain day, the price increases 2% for every protection purchased(except the first 5).
- For flights departing within 24 hours, the price increases 5% for every protection purchased.

The three rules work together, and product this modifier to basic price results to its final price. Such float-pricing system is designed to limit the operating space of inside traders. All kindly users are not expected to be affected, thus some exemptions(from all three rules) are provided accordingly:

- Users who upload their identity information and ticket vouchers can be exempted.
- Users holding 1,000 + DEGIS tokens for 3+ months are exempted.

8.2 Simulation

To verify the effectiveness of our pricing methods, we designed a backtesting system, an agent-based one, for simulating the actions and interactions of autonomous agents to understand the behavior of a system and what governs its outcomes. Three different types of agents are considered here:

- Random Trader: enter this protection pool randomly to buy products at given probability.
- Rational Trader: ask for protections based on his own prediction model.
- Attacker: entitled some certain ability to know the future information, and would buy if current price falls below the expected payout.

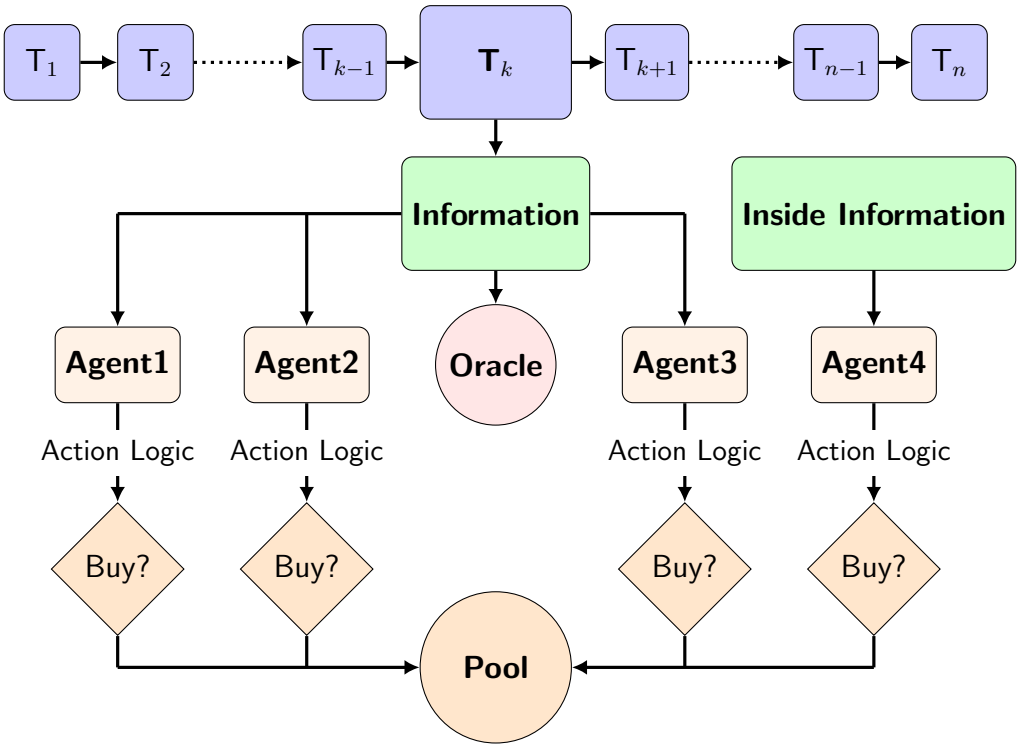

Figure 8.2: Schematic diagram of the back test system. The back test system uses historical data in time series to simulate transactions. All normal agents and the oracle get only the published information, e.g. airline timetable, weather. Inside traders know the exact delay time. Agents will make decisions depending on the information they get and the price that the oracle predicted. If they decide to buy, the order will be put in the pool.

Let us take the flight delay protection as an example to explain further. Under this specific market settings, agents can be described as:

- Random trader: buy with a *base probability* chosen from [0.4, 0.8], and actual buying probability would be adjusted according to protection settings.

$$Actual\ Probability\ = Base\ Probability \times \frac{Days\ to\ Depart}{7} \times \frac{1}{protection\ Price}$$

  i.e. the closer to the departure date and the more expensive ticket will lower the possibility of purchase, which seems to be reasonable.

- Rational trader: use one bench model to help decide. If the protection's expected payout exceeds its price, then it's a deal. Rational users adopt bench model or some smarter ones, while the pricing system uses embedded model. Rational users also would begin trading 7 days before departure.

- Attacker: entitled some certain ability to know the true depart delay, and would buy if current price falls below the expected payout. *Note that attackers can only buy* 3 *days before departure*. The prediction is generated from the uniform distribution of following intervals:

$$[\text{TrueValue} \times \textit{ability},\ \text{TrueValue} \times (2 - \textit{ability})]$$

By adjusting the ratio of attackers to the total number of buyers, we can see the model's performance in different environments. In the following, we present our backtest setup and simulation result.

8.2.1 Data Description

Historical flight data is collected from the Bureau of Transportation Statistics, USA, including airline conditions, flight summary, and time information. The simulation described here involves all American flights information from Jan 2020 to Jun 2021. Our backtest starts from Jan 2021 to not overlap with the model training part, and the pricing model updated accordingly over time.

8.2.2 Basic Statistics

1. Put 5,000 USD in liquidity pool at the very beginning.
2. Set a 2:1 ratio of buyers(RandomTrader & RationalTrader) versus attackers in the market.
3. Run the simulation.

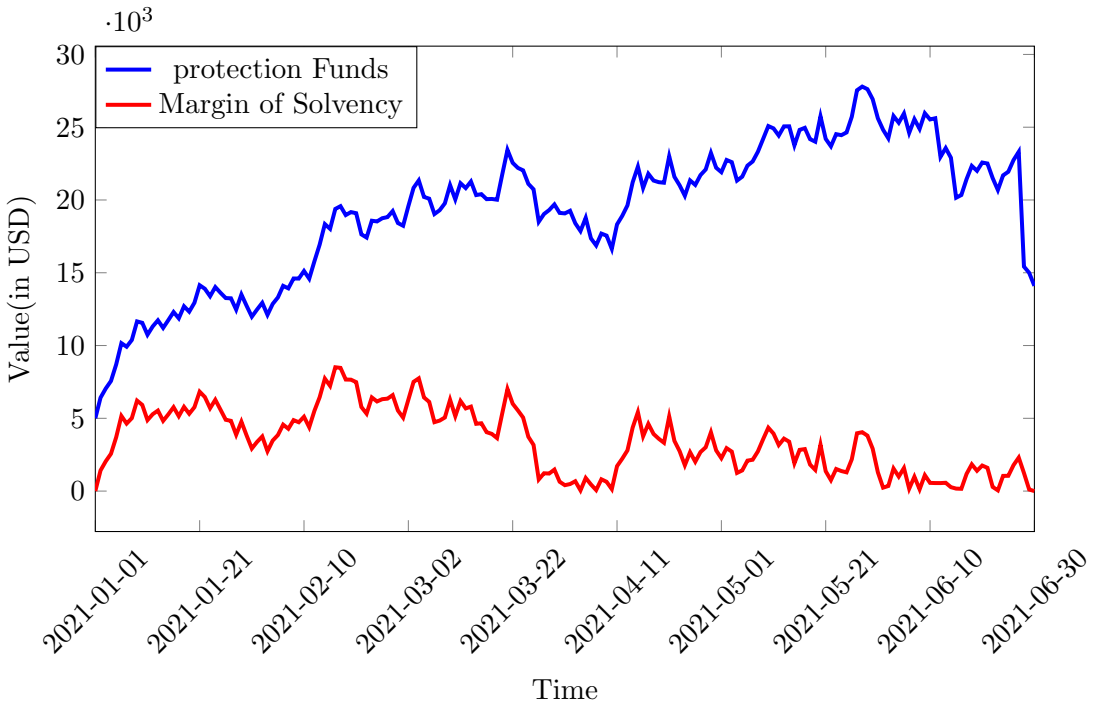

Figure 8.3: protection Funds and Margin of Solvency in pool

The chart (8.3) shows *protection Funds** & *Margin of Solvency** condition in pool, from which we can conclude that our protection pool can grow steadily even with attackers engaged.

Margin of Solvency: margin to meet all potential future payout.*

protection Funds: all capital in pool, including liquidity, undistributed profits, and margin of solvency.*

And several important indicators for protection product are calculated to be:

- Net Profit: 9,100
- Return on Equity: 64.54%
- Claim paying ability: 187%
- Annual Percentage Rate: 167%

8.2.3 Prohibit Inside Trading

(8.4) shows the gross profit ratio of protection products under different attacker ratio, and our break-even line is 50%.

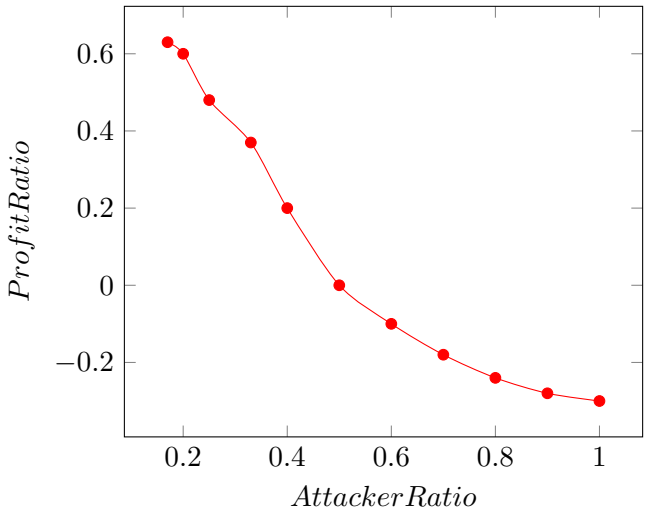

Figure 8.4: Relationship of profit ratio and attacker ratio. Because of the floating price policy, we have a fixed maximum loss on each delay. Even if all the agents are attackers, our loss will not exceed 30% of the pool.

8.3 Data Oracle

8.3.1 Flight Delay

We have multiple reliable data sources for flight information query services and status updates, sources including Cirium, FlightRadar24, FlightStats and Bureau of Transportation Statistics, USA.

8.3.2 Chainlink Oracle

Parametric protection built on top of decentralized infrastructure is one of the most exciting frontiers of innovation in the protection industry. Not only does this protection model foster new product designs and increase market participation, but it redefines underlying trust dynamics between protection providers and policyholders.

Here we use one three-party trustworthy decentralized data oracle service, named Chainlink to update protection status(e.g. flight delay status) information. All claims are transparent on-chain and settled fairly since there would be no information asymmetry.

Chainlink is a decentralized oracle network that gives smart contracts secure and reliable access to data providers, web APIs, etc. We are setting and operating Chainlink nodes to fetch data from trusted web APIs for status-related data.

References

[1] Connor Martin, Callil Capuozzo, The Uniswap V2 Protocol

[2] Friedman, J.H. Greedy function approximation: a gradient boosting machine. The Annals of Statistics, pp. 1189–1232, 2001.

[3] Ravi Myneni, The Pricing of the American Option, The Annals of Applied Probability Vol. 2, No. 1 (Feb., 1992), pp. 1-23

[4] Mark Broadie, Jerome Detemple, American Option Valuation: New Bounds, Approximations, and a Comparison of Existing Methods, The Review of Financial Studies, Volume 9, Issue 4, October 1996, Pages 1211–1250