Blockchain Insurance

Xiao-Bo Li

January 28, 2023

Contents

1 Disclaimer

This document is a proposal. Its contents are subject to change. These ideas are presented as-is, and may have errors.

2 Introduction

Blockchain lending protocols are smart contracts that handle the lending of assets. These protocols use overcollateralization to decrease risk. A similar idea can be used to implement insurance on the blockchain.

Traditional (centralized) insurers use past experience to determine the amount of premium to charge for a given benefit. Benefit payout is handled by people. This entire process can be automated by a smart contract. However, in the case of a smart contract, the premium paid is equal to or more than the benefit to be paid out to ensure the insurer stays solvent.

A smart contract does not have a person examining past data. Rather, a token representing past experience can be issued to the insured. The smart contract can then decrease the premium of the insured based on the amount of experience token the insured pays into the contract.

Insured users who can pay large amounts of experience tokens are good risks which have been with the insurance company for a long time, and which the insurance company wants to keep as customers.

3 Terminology

The **insurer** is the smart contract that provides the insurance by taking in premiums. The insured is the user, or counterparty, wanting to recieve a benefit in exchange for paying a premium to the insurer smart contract.

The **benefit** is the amount the insured receives when the insured makes a claim. The **premium** is the amount the insured pays into the insurer.

Successful centralized insurers keep more premiums than they pay out in benefits to stay **solvent**. If the amount of benefit paid out is more than the amount of premiums taken in at any point in time, the insurer becomes insolvent.

Term is the period of time after premium payment during which a claim can be made. On the blockchain, term can be measured in how many blocks were added since the premium has been paid.

The **insurance contract** is the protocol that determines how much benefit is paid out, and how much premium is paid in, within a specified term.

The insurance contract is different from the **insurer smart contract**, which is the code on the blockchain that implements the insurance contract. The insurance contract is active during the term, whereas the smart contract is always on the blockchain.

4 Benefit

The benefit is the amount the insurer will pay to the insured. This amount can be fixed by the protocol to one or more levels, e.g. 1000 USDC, 10,000 USDC, 1 ETH etc.

Benefit and claim will be used as synonyms in this document.

5 Premium

The premium is the amount the insured will pay into the insurer smart contract. Centralized insurers allow lower premiums to be paid for lower risks. Premium calculation is based on past data.

A smart contract can simulate this risk-adjusted premium and lower the amount of future premium required by issuing to the insured a special token, called the "experience token". Similar to getting cash-back for shopping, the insured can use the experience tokens to pay less premiums in the next term.

6 Reserve

Just as with centralized insurance, the total of all premiums deposited with an insurer is called the **reserve**.

7 Experience Token

Experience tokens are tokens issued by the insurer to reward the insured for being a good risk. Experience tokens can also be used to participate in the insurance company DAO. Large experience token holders have been customers with the insurance company for a long time, and are good risks.

The experience token is not a stablecoin, it has a market value that fluctuates. However, this property can be changed in the future if a stablecoin implementation is better.

8 Experience Token Exchange Rate Risk

The insurer will not hold experience tokens, only issue them to the insured. This way, if the experience tokens become worthless, the insured's premiums still have value and can be used to pay benefits and claims.

An insurer will choose one cryptocurrency for holding its premiums and paying out benefits, this cryptocurrency is called its **base currency**.

There is always the risk that the experience token, or any of the other cryptocurrencies become worthless.

9 The Central Idea of Insurance

The central idea of traditional insurance is the insured is willing to suffer small predictable loss in exchange for a large unlikely and unpredictable loss.

The small predictable loss is the premium the insured pays to the insurer. The insurer pays the large unlikely unpredictable loss. The law of large numbers changes this payout to a predictable small loss for the insurer.

The central idea of distributed insurance is the same for the insured. For the insurer, it uses overcollateralization to decrease insolvency risk, and issues experience tokens to lower the cost of insurance for good risks.

10 A Distributed Insurance Protocol

This section proposes how a smart contract can automate the function of an insurer. Note the similarities of this insurance protocol with other overcollateralized lending protocols.

Insurance contracts have a term. On the blockchain, this term can be measured in the number of blocks since the premium was paid into the insurer. For example, after 5 blocks are confirmed, the insurance term can end. After that, premium must be paid to the insurer again to stay insured.

A longer term has higher risk, so the premium charged should also be higher. Let the term of the insurance contract be denoted by T.

In the following discussion, suppose the premium is $p = 1000$ USDC and the benefit is $B = 900$ USDC.

Suppose at time t_0 an insured wants to open an insurance contract which provides 900 USDC in benefit during the term. The insured deposits funds into the insurer smart contract. In order to ensure there is enough money in the insurer, the insured must "overpay", similar to overcollateralized lending protocols. Let p denote the premium paid at the beginning of the insurance contract term, and B denote the one benefit paid during the term of the contract. The following relation must hold:

$$p \geq B \ .$$

Let t_1 be the next point in time during the term of the insurance contract, $T \geq t_1 > t_0$. If the insured wants to make a claim, the benefit amount of 900 USDC is paid out, leaving the premium amount of 100 USDC with the insurer. The insurer is solvent and profitable after this transaction with a reserve of 100 USDC.

Suppose the insured does not make a claim, and the insurance contract expires at $t_2 \geq T$. The entire premium amount of 1000 USDC is kept by the insurer. In order to reward the insured for not making a claim, the insurer issues experience tokens to the insured equal to the amount of the benefit, 900 USDC. The insurer now has a reserve of 1000 USDC.

Topics of further research include when should the experience tokens be minted, whether the experience token can be bought and traded in other markets, whether there should be a fixed supply of experience tokens.

Since the insurance contract has expired at time T, after this time, the insured needs to make another premium payment to stay insured. This time, the insured has a choice in how they pay the premium.

- Overpays the benefit as before, 1000 USDC.

- Convert the experience token to 900 USDC, then added another 100 USDC to give a total of 1000 USDC, which then is used to overpay the benefit. Note the market value of the experience token can fluctuate.

During this next term, if the insured does make a claim, 100 USDC is kept by the insurer and added to its reserve. 900 USDC is paid out. But if the insured does not make a claim, then again they get back experience tokens. The experience tokens paid back to the insured is based on the 900 USDC benefit value. In this case 1000 USDC is added to the reserve.

As long as the insured does not make a claim, they will end up paying the small premium. This premium is the small predictable loss they are willing to suffer in exchange for an unlikely future benefit payout.

The insured should keep in mind that the amount of experience tokens paid at the beginning of the term, and the amount received back at the end of the term can be different due to changing exchange rates. Recall the insurer will hold USDC and not experience token, this is the reason this risk is off-loaded to the insured.

If the insured is always willing to pay 1000 USDC out-of-pocket, and not exchange the experience tokens, then good risks will in the long run be holding a large amount of experience tokens. and will find the insurance cost is getting cheaper and cheaper. The experience token's market value may also increases to further offset the cost of buying insurance.

The insurer will have a larger reserve when it insurers more good risks compared to when it insurers more bad risks. This large reserve is entirely the profit of the insurer since premiums always overpay the benefits.

The above example uses USDC as the base currency, but insurers with base currency in many cryptocurrencies can be created.

11   Conclusion

This document proposed a distributed insurance protocol which can be implemented on a blockchain. The protocol is inspired by other defi protocols, such as overcollateralized lending and automatic market making. The general ideas used are locking up assets, and issuing tokens. The idea of this protocol is that the insured pays small predictable losses called the premium, and gets back the benefit or experience tokens. The insurer does not hold experience tokens, but can hold any other cryptocurrency as its reserve, which is called its base currency.