BLOCKSURANCE DAO

A decentralized insurance protocol on the Ethereum blockchain.

ALEXEI MIRKIN

ABSTRACT

The insurance industry has been very slow to adapt to new possibilities within the now thriving digital assets space. This space is also riddled with security problems, which presents a tremendous opportunity. BLOCKSURANCE uses blockchain technology to bring our users the ability to secure their DeFi assets while earning rewards by creating smart contract vaults with incentives through Solidity code on the Ethereum blockchain.

Introduction

Decentralized finance (DeFi) has experienced tremendous growth recently. In 2013, renowned crypto expert Vitalik Buterin, published the Ethereum Whitepaper[1], which described the a next-generation of decentralized applications and a smart contract platform. A year later in 2014, Buterin raised over $18 million in an ICO, and by the end of 2021, the total market cap of Ethereum has reached to a staggering $550 billion. This meteoric rise of the Ethereum ecosystem can be attributed to both the technology and the philosophy of the platform. They have shown us that offering decentralized financial services at scale is possible.

Ethereum has so far captured the minds of crypto enthusiast and investors seeking for an alternative to centralized finance. Today, the vast majority of users and developers within the blockchain space are focused on Ethereum. According to data sourced from Consensys, there are more than 200,000 active Ethereum developers and the network hosts over 4x more developers than any other crypto platform.

In this piece, we shall be considering the impacts of the ERC20[7] standards on the Ethereum ecosystem. Focus will also be given to the potential security problems related to Solidity and some recent high-profile hacks that resulted from the use of such smart contracts. We will also have a detailed look at our own “2x10” protocol, which allows us to provide force majeure coverage to BLOCKSURANCE users.

Impacts of the ERC20 Standards on the Ethereum Ecosystem

The Ethereum Request for Comment (ERC20)[7], is a token standard utilized within the Ethereum ecosystem. The standard was implemented in 2015, and it signifies the number of actions and rules than an Ethereum smart contract must follow, together with the steps needed to execute it. It can simply be defined as the fundamental functions and guidelines a newly created token within the Ethereum must include. Lots of popular cryptocurrencies utilize the ERC20 standard including ApeCoin (APE), Maker (MKR), OMG Network (OMG) and Augur (REP). It was popularized by PancakeSwap and the Uniswap protocols[6], which provide users the ability to swap various ERC20-based tokens for one another. Both platforms are DEX protocols that are built on the Ethereum network.

Since its introduction, the ERC20 standard has risen to become the major pathway for the development of new tokens within the cryptocurrency space. It has been remarkably popular with crowdfunding and ICOs companies. There are presently thousands of unique tokens that have been released.

Finally, ERC20 standard set of functions can be used to monitor fungible tokens.. This makes ERC20-based tokens vital for things such as voting rights, staking, as a means of currency exchange and lots more.

Potential Security Problems Associated with ERC20 Standard

Despite the many utilities and values of the ERC20 standard, there are however, some potential risks associated with it that need to be highlighted. Firstly, Ethereum has a low scalability issue that leads to high gas fees resulting to very costly transactions. Even little transactions become expensive due to this problem making it highly unsustainable for users. Another direct consequence of Ethereum's low scalability is the slow nature of transactions on the platform.

Furthermore, in recent years, we have witnessed a number of notorious security incidents concerning the Ethereum blockchain that resulted in significant financial losses or drastic measures being taken to avoid the consequences. [2,3]

Introduction of Ethereum 2.0 is set to resolve these issues; however, pending the full launch, there will also be risks associated with the use of the ERC20 standard.

High Profile Hacks of the ERC20 Smart Contracts

Vulnerabilities have been recurrent within the history of the Ethereum network and smart contracts built on the ecosystem have witnessed a number of hacks. Some of such top hacks include:

The DAO Hack

DAO is a decentralized autonomous organization (DAO)[5], launched on the Ethereum network in 2016. The fund's Ether value as of 21 May 2016 was more than US$150 million from 11,000 investors. On June 18th 2016, the DAO was hacked as a result of vulnerabilities within the code base and over $60 million was lost [4]. Following the hack, the Ethereum blockchain underwent a hard fork to help restore the stolen funds. However, not all parties involved were in agreement with the decision, and this resulted in the breaking up of the network into two unique blockchains: Ethereum Classic and Ethereum.

The Beanstalk Hack

Beanstalk is a credit-focused protocol built on Ethereum. On April 17th, 2022 it was discovered that around $182 million had gone missing following a flash loan attack. The hacker(s) laundered over $80 million Ethereum through Tornado Cash. Beanstalk is renowned for its algorithmic stable-coin called BEAN, which is designed to have a value of $1. While the platform managed to hold its ground following the attack, the hack however, demonstrates that algorithmic stable-coins are just as stable as the smart contracts they are built upon. It's just the latest in a string of crypto heists in the last year totaling well over $2 billion.

Other top Ethereum-based hacks include:

- The Parity Wallet Hack worth $30 million
- The Ronin Hack worth over $550 million
- Ethereum Parity Wallet Freeze worth $280 million

Decentralized Exchanges and Liquidity Providers

The return of a liquidity provider between time $t1$ and $t2$ in percent is given as

$$\text{return}_{t_1 \to t_2} = 100 \cdot \frac{\frac{\text{invest}_{t_2}}{\text{hold}_{t_2}} - \frac{\text{invest}_{t_1}}{\text{hold}_{t_1}}}{\frac{\text{invest}_{t_1}}{\text{hold}_{t_1}}},$$

where invest t , which is the current value in USD of the liquidity placed in the pool at time t and hold$t$ is the value in USD of the constant-mix portfolio at time t. [8]

Consider a liquidity pool A $\rightleftharpoons$B between token A and B, where the amount of A in A $\rightleftharpoons$B at time t is denoted as At and the amount of B in B $\rightleftharpoons$A at time t is denoted as Bt. The fees collected between time $t1$ and $t2$ as a percentage of the liquidity are given as,

$$\text{fees}_{t_1 \to t_2} = 100 \cdot \left(1 - \frac{\sqrt{k_{t_1}}}{\sqrt{k_{t_2}}}\right),$$

where kt = At · Bt [9].

BLOCKSURANCE 2x10 Decentralized Insurance Protocol

Tokens and their underlying protocols are vulnerable to external and internal threats. In accordance with our terms of service[10], we are offering automatic force majeure coverage on tokens deposited into individual token vaults created by users on the platform. The fee structure is defined as follows:

- 0.005 ETH vault creation fee
- 2% commission on token deposits into vaults
- Stake in $4SURE Coin that represent at least 10% of the vault value

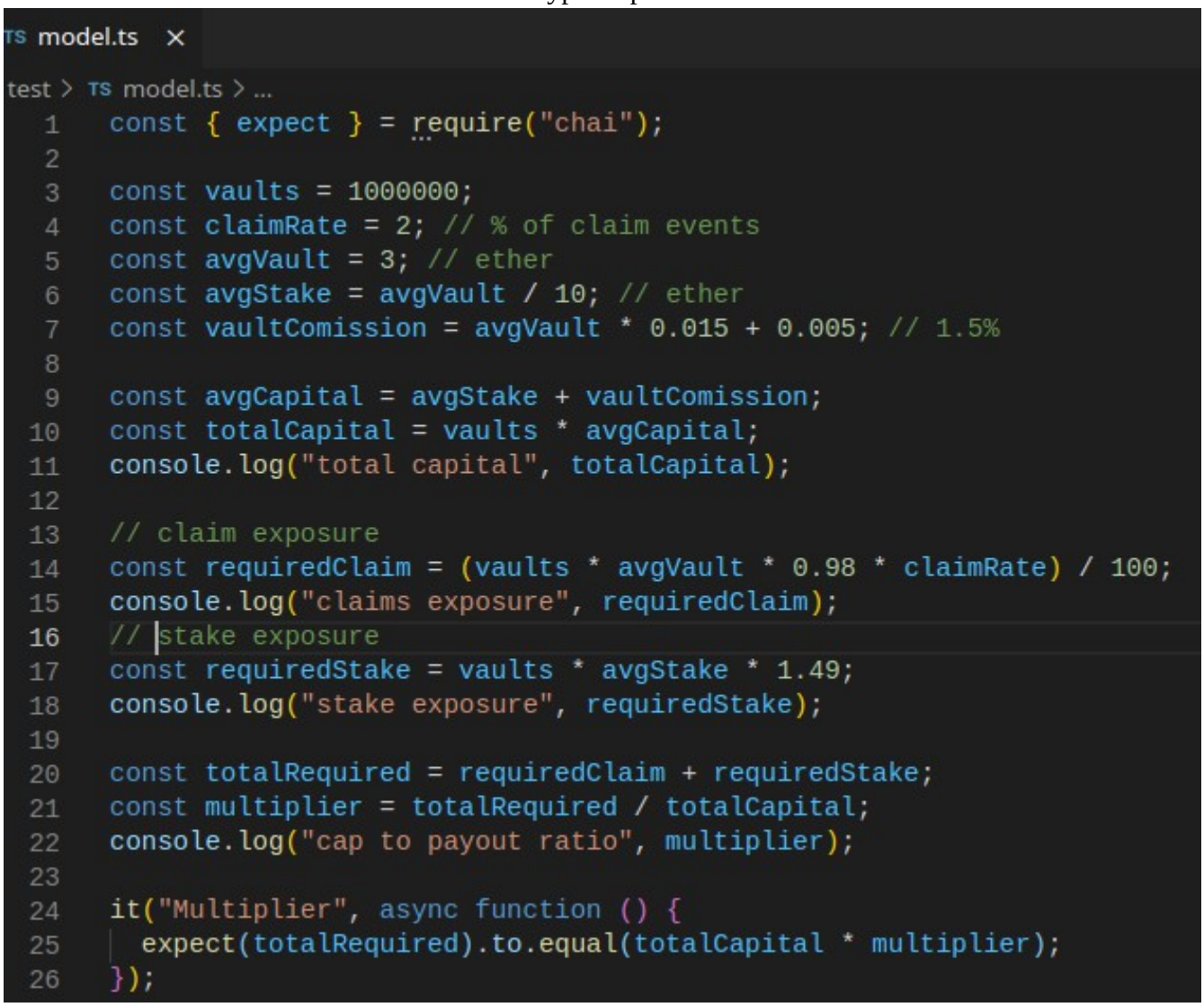
The inner workings of the protocol are as follows: fees and stakes obtained by the platform are routed into DEX liquidity pools via the mechanism that is approved by the BLOCKSURANCE DAO, which is publicly available via snapshot.org[11].

We have created various mathematical models to simulate the outcomes of such activity to test our levels of exposure. Lets examine an example case which we believe represents the worst case scenario for BLOCKSURANCE. The variables involved are as follows:

- Number of vaults: 1,000,000

- Vault creation fee: 0.005 ETH
- Average Stake Value: 0.3 ETH
- Average Vault Value: 3 ETH (10x Stake)
- Claim rate: 2%
- Staking APR: 45%
- Staking Referral Bonus: 4%
- Vault commission minus referral commission: 1.5%

We have created a basic test for this case with typescript:



Which creates the following output:

```
> hardhat-test3@1.0.0 test
> hardhat test

No need to generate any newer typings.
total capital 350000
claims exposure 58800
stake exposure 447000
cap to payout ratio 1.445142857142857


  ✓ Multiplier

  1 passing (3ms)
```

As you can see, in order to break even from the worst case scenario, we need to achieve a ~45% return on capital obtained by the platform via commissions and staking. If you are familiar with DEX operations, then you should know this is easily attainable by liquidity providers.

The benefits to our users are obvious. They get to earn value while keeping their assets safe. Let further break down this example from the perspective of user exposure.

In the event of no claim:

- total commissions paid: 0.005 + 0.06 ETH
- gas fees: ~0.02 ETH
- return from staking: 0.135 ETH
- tokens returned

In the event of a claim:

- total commissions paid: 0.005 + 0.06 ETH
- gas fees: ~0.02 ETH
- return from staking: 0.135 ETH
- value recovered: 2.94 ETH

As you can see, the user is earning value thanks to the protocol in both scenarios, while keeping the digital assets protected from a force majeur. This is the “earn while you're safe” concept from BLOCKSURANCE.

References

[1] Ethereum whitepaper by *Vitalik Buterin*. Retrieved from https://ethereum.org/en/whitepaper/

[2] *N. Atzei, M. Bartoletti, T. Cimoli*, A survey of attacks on Ethereum smart contracts: https://doi.org/10.1007/978-3-662-54455-6_8

[3] *Simon Joseph Aquilina, Fran Casino*, EtherClue: Digital investigation of attacks on Ethereum smart contracts: https://www.sciencedirect.com/science/article/pii/S2096720921000233

[4] *G. Prisco*, Understanding the DAO attack, Accessed: 2021-01-12 (2016), https://bitcoinmagazine.com/articles/the-dao-raises-more-than-million-in-world-s-largest-crowdfunding-to-date-1463422191

[5] *Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times. Archived from the original on 2016-05-27.*

[6] Uniwsap v3 Whitepaper: https://uniswap.org/whitepaper-v3.pdf
[7] Ethereum Improvement Proposal: https://eips.ethereum.org/EIPS/eip-20 , 2015

[8] *Lioba Heimbach, Ye Wang*, Behavior of Liquidity Providers in Decentralized Exchanges: https://arxiv.org/pdf/2105.13822.pdf
[9] *Hayden Adams, Noah Zinsmeister, and Dan Robinson.* 2020. Uniswap v2 Core. (2020).
[10] BLOCKSURANCE Terms of Service: https://blocksurance.io/termsandconditions.pdf
[11] Snapshot DAO Management platform: https://snapshot.org