Security/Privacy/Scalability issues in Title of Your Development Project

Chan Geng Tat  
U1821992D   
*School of Computer Science and Engineering*  
*Nanyang Technological University*Singapore  
chan0886@ntu.edu.sg

Poh Jun Rong  
U18  
*School of Computer Science and Engineering*  
*Nanyang Technological University*Singapore  
jpoh015@ntu.edu.sg

Cecelia Soh Yan Pei  
Student’s Matriculation Number   
*School of Computer Science and Engineering*  
*Nanyang Technological University*Singapore  
C190013@ntu.edu.sg

*Abstract*—This is the term paper of CE/CZ4153 Blockchain Technology course offered at the School of Computer Science and Engineering, Nanyang Technological University, Singapore. This paper is to present the issue out of the Security, Privacy and Scalability in WardWard’s Trade Mining Rewards Project. The project develops a decentralized application to assign token rewards to users for each transaction they make on Pendle’s AMM. (Summary…)

Keywords—Blockchain, Ethereum, smart contracts, tokens,

# Introduction

Blockchain technique is widely used in the financial transaction system. The basic logic of blockchain technology is to duplicate and distribute a digital ledger of transactions across the entire network of computer systems on the blockchain. The transactions on the blockchain are recorded and encrypted with hash, which is an immutable cryptographic signature. By doing so, the recorded information of the ledger is challenging to change and hack. If there is an on-chain block change, the hash value of the block will also be changed, and it is different from the value recorded on the next block. Therefore, it is apparent that the block had been tampered with. If the adversary wants to control or corrupt a blockchain system, they need to change every block in the chain, which has been distributed. Nowadays, blockchain technologies have become an indispensable technique in Decentralized Finance (DeFi).

Several prominent issues have been regarded when developing DeFi with blockchain techniques, including Security, Privacy and Scalability.

1. Security – A blockchain application is built by several layers, which consist of data layer, network layer, consensus layer, incentive layer, contract layer and application layer. We need to pay more attention to the security problem on some layers because some malicious parties can easily control the blockchain by hacking on the network layer, consensus layer or the smart contract layer. At the consensus layer, they can bring down the security threshold by Selfish Mining and make the Frontrunning Attack, which reduces the security on the consensus layer. Eclipse attack on the network layer can cause the 51% attack and double spending problem. These two problems are the most taboo issues in the blockchain. When creating a smart contract, we should review the overflow & underflow bug and reentrancy bug to prevent weakening the security during transactions
2. Privacy – As the ledger of transactions is distributed to every node, hence, the user’s personal privacy should be protected. To avoid divulging users’ information, the characteristic of anonymity of users’ identity and the unlikability of transactions in blockchain is indispensable. The methodology to achieve these includes clustering addresses, CoinJoin, Monera, Zerocash and so on.
3. Scalability – The continuously increasing the number nodes on-chain has resulted in the problem of handling and storing a large quantity of transaction data in the blockchain. The solution to date is to random split into the chain to multiple shards to avoid creating adversarial networks and reducing the security. Elastico/ Zilliqa Sharding and NearProtocol Sharding are the two protocols of sharding to solve the on-chain scalability problem and avoid resulting the security problem. In addition to the on-chain solution, there are several off-chain solutions include the Channel-based networks method and the Commit-chains method, which ensure the data availability and state validity.

Our development project is to create a decentralized application to reward PENDLE tokens to users for each transaction they make on Pendle’s AMM. Pendle is a protocol that provides users to tokenize their future yield on an AMM system and sell these tokens to lock in the current interest rates for upfront cash. To provide liquidity to Pendle, the holder of yield-generating assets can deposit the tokens into Pendle’s AMM, and hence they are also liquidity providers. Incentives would be returned to them. The transactions done in Pendle’s AMM are fully on-chain because they all are handled by smart contracts and are verifiable. Automated market maker (AMM) is a type of decentralized exchange (DEX) protocol that uses a mathematical formula to calculate asset price. The mathematical formula can vary from protocol to protocol. Pendle’s AMM has its own mathematical formula to mint the token:

, where x and y are the amounts of two swap tokens, k is defined as the liquidity of the pool and α represents the curve shift of the x, y exchange equation.

The gas fees increase when the number of transaction block increase; the average daily gas price nowadays have been up to a nasty amount of 200 gwei. There is an obscene overhead for the users. To help the user reduce undesired spending, we designed a system to distribute rewards to trade mining users retroactively. To accomplish this, we build a new smart contract called TradeMiningRewards, which is triggered when a transaction happens. Our application is able to collect and record the trade mining participants of the Pendle Market and the reward Token. The system can also calculate the return amount by a simple formula: . The incentive Token will return back to all verified participants once every two weeks.

# Motivation and Literature Survey

## Motivation

In this subsection, you should clearly argue which one of the three issues – Security, Privacy, Scalability – concerns you the most in case of the Decentralized Application you developed. You may refer to the lectures, invited talks, related works, or any other instance of similar development projects to argue this.

## Literature Survey

Term Paper submitted for CE/CZ4153 Blockchain Technology course, NTU.

In this subsection, you should carefully curate similar works in the area of your interest, with proper citation (see references). This may include similar development projects or decentralized applications that have faced the same issues, lectures, articles, books or papers that talk about the issue in your case, or any other academic material related to your specific case.

# Observations and Analysis

In this section, start by listing your main observations on the issue you chose in case of your development project. In each case, discuss the major considerations, analyze their impact (and ramifications) on your decentralized application, and compare it with similar cases in the literature, if you found any such case.

## Issue X in case of Component I

Identify the specific issue X that will affect component Y of your decentralized application (e.g., *re-entry bug in case of the auction contract*). State why you think this issue may occur, what would be the impact on your application, and whether you know of any similar case in the literature where this happened.

## Issue Y in case of Component I

There may be more than one issue per component. Think carefully to spot all such issues in your development project and write one subsection on each one of them. In case they are connected, do mention that too in this portion of your paper.

## Issue Z in case of Component II

There may be more than one component with an issue. Think carefully to spot all such issues in your development project and write one subsection on each one of them. In case they are connected, do mention that too in this portion of your paper.

# Proposed Solutions

In this section, propose potential solutions to address the issues that you found in your analysis earlier. These solutions may be inspired from the lectures, invited talks, related works, or any other instance of similar development projects.

## Solution to Issue X

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project.

## Solution to Issue Y

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project. In case the solution to issue X already solves Y, mention that.

## Solution to Issue Z

Identify potential solutions to this issue. Clearly mention how you would apply the solution to your development project, and if you have already applied the solution. Applying the solution is of course not mandatory for the development project. In case there exists no known solution to issue Z, propose a potential solution on your own, and argue why it may work.

# Conclusion

In this section, you should mention exactly which issue out of the three – Security, Privacy, Scalability – you presented, and what is the overall contribution of this paper. The contribution may be in terms of your observations, analysis or proposed solutions presented for the issues and the components.

You may follow the IEEE paper format for the Tables, Lists, Figures, References, etc. Keep the format uniform in the paper.

##### References

1. A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder, “Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction,” Princeton University Press 2016.
2. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” IEEE Symp. on Security and Privacy 2015: 104-121.
3. I. Eyal and E. Gun Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” Financial Cryptography, 2014, pp. 436–454.