Project Report

Time Locked Pension

Submitted By

Anjali Singh Tisha Madame

(2023JCS2565) (2021MCS8340)

Submitted To

Prof. Subodh Vishnu Sharma

INDIAN INSTUTUTE OF TECHNOLOGY, DELHI

Content

1 Introduction

The TimeLockedPension contract is a decentralized application (dApp) deployed on the RemixVM environment. It aims to provide a secure and transparent platform for managing pension funds with time-locked withdrawals. This report provides a comprehensive overview of the contract's structure, functionality, security considerations, and recommendations for improvement.

2 Contract Structure

The TimeLockedPension contract is structured to facilitate the following key functionalities:

1. **Owner and Unlock Time**

   The contract records the address of the owner, who has privileged access rights, and the unlock time, which specifies when the funds become available for withdrawal.

2. **Balances Mapping**

   It utilizes a mapping data structure to associate user addresses with their respective balances, enabling seamless tracking of deposited funds.

3. **Events**

   The contract emits Deposit and Withdrawal events to provide transparent logging of user transactions on the blockchain.

4. **Modifiers**

   - **onlyOwner -** Restricts certain functions to be accessible only by the contract owner, ensuring secure access control.
   - **afterUnlockTime -** Ensures that specified functions can only be executed after the unlock time has been reached, preventing premature withdrawals.

3 Contract Functions

The TimeLockedPension contract offers the following functionalities to users:

1. **Deposit**

   Users can deposit funds into the contract by invoking the deposit function. Deposited amounts are added to the caller's balance, facilitating easy fund management.

2. **Withdraw**

   The contract owner can initiate fund withdrawals after the unlock time has elapsed. The withdrawal function enables the owner to specify the amount to withdraw, subject to certain constraints such as sufficient contract balance.

3. **Get Balance**

   Users can query their account balances using the getBalance function, providing transparency and visibility into their deposited funds.

4. **Receive Function**

   The contract implements a receive function to handle incoming ether transfers. While currently empty, this function can be leveraged to perform additional actions or logging.

4 Working of Time Locked Pension

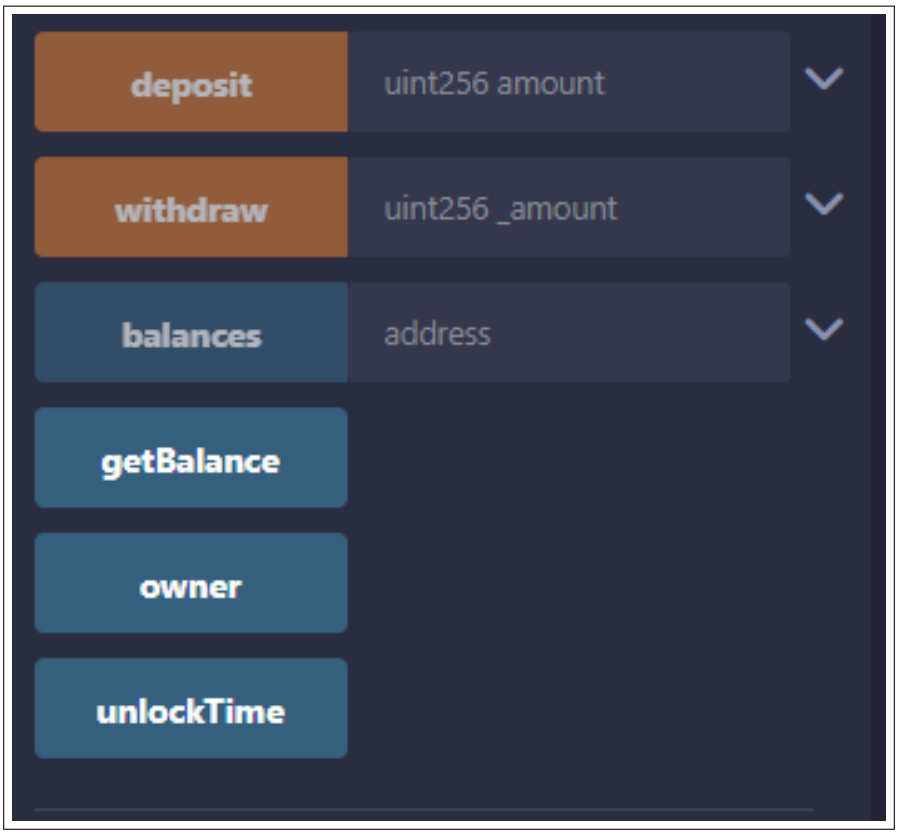

Figure 1: A snapshot of Remix tab when we have just compiled our solidity Code.

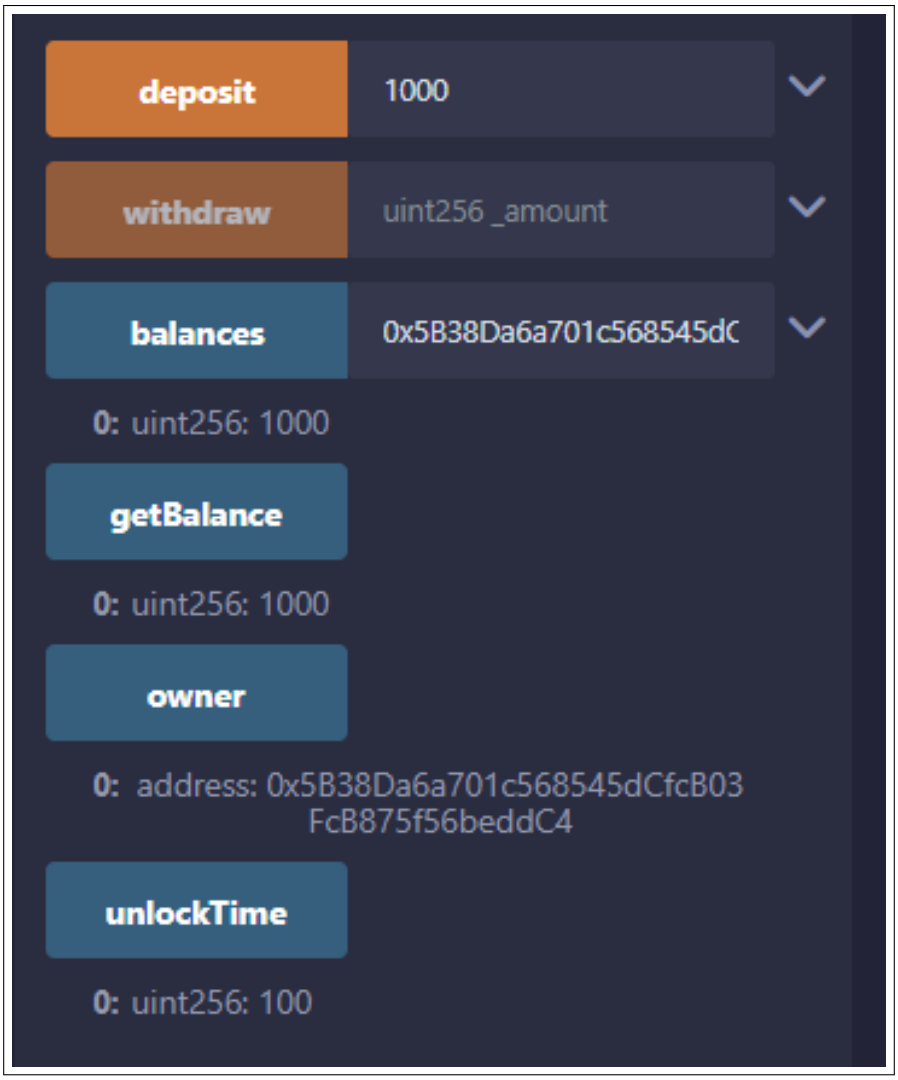

Figure 2: A snapshot of Remix tab when we have ran shown functions in our solidity Code.

Figure 2 illustrates key functionalities such as **Balances** which displays the current balances of various accounts, **getBalance** function which retrieves the balance of a specific account when provided with its address, **owner** function which determines the owner of a particular account, **unlockTime** function which indicates the time at which locked funds in an account become available for withdrawal.

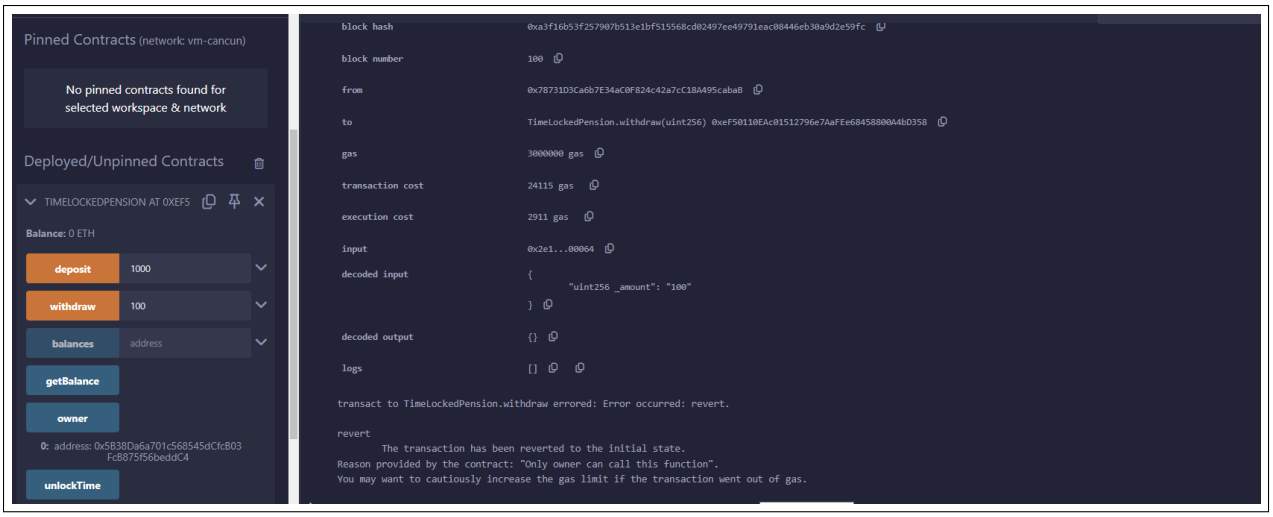

Figure 3: A snapshot of Remix tab when we tried to withdraw using a account different from the owner and it showed error.

The owner's account address displayed in Figure 3 (left tab, below the "owner" function) doesn't match the account number attempting withdrawal (indicated by "to"). This discrepancy ensures that only the owner can withdraw funds.

5 Security Considerations

The TimeLockedPension contract prioritizes security by implementing the following measures:

1. **Modifiers and Require Statements**

   The contract employs modifiers and require statements to enforce access control and validate inputs, reducing the risk of unauthorized access and erroneous transactions.

2. **Fallback Function**

   While not currently utilized, the contract includes a fallback function to handle unexpected ether transfers, mitigating potential vulnerabilities.

6 Conclusion

The Time Locked Pension contract presents a robust solution for managing pension funds with time-locked withdrawals on the Remix VM environment. With its secure architecture, transparent functionality, and potential for further enhancement, it offers a promising platform for decentralized pension fund management. By addressing the recommendations outlined in this report, the contract can evolve into a versatile and reliable tool for pension fund administration in the decentralized finance (DeFi) ecosystem.