DeFi - FlashLoan

Ivan Sendin

FACOM - Universidade Federal de Uberlandia
ivansendin@yahoo.com,sendin@ufu.br

15 de outubro de 2024

- DeFi
- AMM - Pool de liquidez
- Front Running
- Reentrancia

- Empréstimos exigem garantias de pagamento
- Carro, casa, consignado,...
- Token

- Os contratos fiam "parados"
  `sleep()`
- Um EOA inicia uma transação
  Chamada de função
- Uma sequencia complexa de chamadas entre contratos ocorre
- A transação termina
- Os dados são armazenados
  Variáveis, saldo, log das transações

- Qualquer envolvido pode invocar um rollback
- `require()` `revert()`
  require-revert-assert e estruturas de controle
- Aquela transação nunca existiu!!!
  ok...gas e log(?)

```
    if (life.badDecision()) {
      revert(``Desculpa ai!'');
    }
}
```

- US$ 100 milhões por dia
  0.09%
- Empréstimos sem garantias (uncollateralized lending)
  Collateral = garantia
- Sem paralelo no mundo tradicional!

- O nome flash vem da velocidade
- O processo ocorre em uma unica **transação**
- Emprestimo, investimento, pagamento do emprestimo+juros
- Se não der certo...`revert()`

Usado, por exemplo, em **arbitragem**

- EX1 vende um token por R$100
- EX2 compra o token por R$102
- Eu tenho R$100
- Compro na EX1,vendo para EX2
- E lucro R$2

Alavancando os lucros com **Flash Loan**

- EX1 vende um token por R$100
- EX2 compra o token por R$102
- Eu pego R$100.000 de empréstimo
- Compro 1000 unidades na EX1
- Vendo 1000 vendo para EX2
- E lucro bruto de R$2000
- Pago R$100.000 + R$1000 para o contrato de FlashLoan
- Lucro R$1000

- Sem riscos para mim
  gas
- Nem para quem fez o empréstimo
- E se eu não conseguir vender na EX2?

```
contract ERC20NaiveBet {
ERC20 t;

constructor(address _t) public {
  t = ERC20(_t);
}

function bet(address player) public returns (bool){
  if ( uint256(blockhash(block.number-1)) % 2 ==0) {
    t.transfer(player,100);
    return true;
  }
  t.transferFrom(player,address(this),100);
  return false;
}

function getAddress() public returns (address) {
  return address(this);
  }
}
```

```
contract ERC20Bank {
 IERC20 t;

 constructor(address _t) public {
   t = ERC20(_t);
 }

 function doFlashLoan(address _b, uint amount)  public {
   FlashBorrower b = FlashBorrower(_b);
   uint256 prevBalance = t.balanceOf(address(this));
   require (prevBalance >= amount,"Not enough funds");
   t.transfer(address(b),amount);
   b.executeFlashLoan(address(this));
   require( t.balanceOf(address(this)) > prevBalance,"Loan Failed");
 }
}
```

```
interface FlashBorrower {
   function executeFlashLoan(address b) external;
}


contract ERC20Borrower is FlashBorrower {

  ERC20 t;
  ERC20NaiveBet nb;

  constructor(ERC20NaiveBet _nb, address _t) public {
    nb = _nb;
    t = ERC20(_t);
  }

  function executeFlashLoan(address b) external override {
    // Estou apostando...mas poderia ser uma arbitragem DeFi
    t.approve( nb.getAddress(),100);
    if (nb.bet(address(this))) {
      t.transfer(b,101);
    }
  }

}
```

```
def main():

    token = ERC20.deploy("TOKEN","TK",10000,{'from': accounts[0]})

    bank = ERC20Bank.deploy(token.address,{'from': accounts[0]})

    token.transfer(bank.address,5000)

    nb  = ERC20NaiveBet.deploy(token.address,{'from': accounts[0]})
    token.transfer(nb.address,5000)



    br = ERC20Borrower.deploy(nb,token.address,{'from': accounts[0]})


    try:
        bank.doFlashLoan(br.address,100,{'from': accounts[0]})
    except:
        print("falha no doLoan")

    print(token.balanceOf.call(bank.address))
    print(token.balanceOf.call(br.address))
```

```
Transaction sent: 0x1dc7d005e7a338bc61832b33c75e310a5cd281ed251a1f576a7c8c354a70df34
  Gas price: 0.0 gwei   Gas limit: 6721975   Nonce: 6
  ERC20Bank.doFlashLoan confirmed (Loan Failed) - Block: 7   Gas used: 150911 (2.25%)

falha no doLoan
5000
0
Terminating local RPC client...



5001
99
Terminating local RPC client...
```

Arbitragem

- Transacao
- Emprestimo de 2.048M de USDC em DyDx
- Comprou 2.028M DAI em Curve Y (cotação 1.010)
- Vendou 2.028M DAI em Curve sUsD (cotação 1.018)...
- Obtendo 2.064M de USDC
- Pagou o Emprestimo em DyDx
- Ficou com 16k USDC

Tudo isso em uma transação

- Transacao
- Pump Attack & Arbitrage
- Manipula o preço em uma DeX usando FlashLoan
  Lembre-se do AMM
- Oracle Manipulation
  Parecido...

tracking the DeFi Ecosystem with Flash Loans for Fun and Profit