



# Verify, don't trust

Being a responsible signer

Santiago Palladino

@smpalladino

# Hey, can you sign this..?

[illegible]



Inspecting

# Understanding the transaction

② Transaction Hash: 0x58916d9727bf9f74f73d3da17f37f127a97ee4017f9d1f2ad66d80f2d5ed93c7

② Status: Success

② Block: 7724203 1 Block Confirmation

② Timestamp: 5 secs ago (Oct-06-2022 09:52:48 PM +UTC)

② From: 0xe3d450f1c50757ffb2b5dde03a1a0d7bc32f0153

② To: Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d

② Value: 0.02 Ether (\$0.00)

② Transaction Fee: 0.001077440041050464 Ether (\$0.00)

② Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 37 Position In Block: 2

② Input Data: 

```
Function: swapExactETHForTokens(uint256 amountOutMin,  
address[] path, address to, uint256 deadline)  
  
MethodID: 0x7ff36ab5  
[0]:  
0000000000000000000000000000000000000000000000000000000000000024  
6139ca800  
[1]:  
0000000000000000000000000000000000000000000000000000000000000000  
0000000080  
[2]:
```

# What's in a transaction?

**to:** who are we calling

**data:** with what

**value:** and with how much eth

## swapExactETHForTokens

```
function swapExactETHForTokens(uint amountOutMin, address[] calldata path,  
    external  
    payable  
    returns (uint[] memory amounts);
```

Swaps an exact amount of ETH for as many output tokens as possible, along the route determined by the path. The first element of path must be [WETH](#), the last is the output token, and any intermediate elements represent intermediate pairs to trade through (if, for example, a direct pair does not exist).

Name	Type	
<code>msg.value</code> (amountIn)	<code>uint</code>	The amount of ETH to send.
<code>amountOutMin</code>	<code>uint</code>	The minimum amount of output tokens that must be received for the transaction not to revert.
<code>path</code>	<code>address[]</code> <code>calldata</code>	An array of token addresses. <code>path.length</code> must be $\geq 2$ . Pools for each consecutive pair of addresses must exist and have liquidity.
<code>to</code>	<code>address</code>	Recipient of the output tokens.
<code>deadline</code>	<code>uint</code>	Unix timestamp after which the transaction will revert.

What's in a proposal?

**to:** who are we calling

**data:** with what

**value:** and with how much eth

...

7B91A5ded31805e42b2208d6  

1D1762F925BDADdC4201F984  

06  



Simulation

Simulate the transaction



# How to simulate a tx?

**Tenderly**


**Defender**


**Blocknative** (API only)

**Ready to execute**

You may now execute this proposal.

Approved 1/1

 0xe3d4...0153

 **Simulate proposal**

**Execute**

**Reject**

**Execute transaction** Goerli ×

This action will execute this transaction.

Transaction nonce:  
**1**

Estimated fee price

**0.00512 GOR** ▼

Advanced parameters

▼

Transaction validity

**Simulate**

You're about to execute a transaction and will have to confirm it with your currently connected wallet.

Cancel **Submit**



# What to look for?

## Contracts involved







## State changes


**Events:** transfer, approval, roles, ownership, upgrades, etc

PROPOSAL SIMULATION RESULT

Block #7,727,774 - 7 October 2022, 13:36 pm (+01:00)

Token Transfers

TOKEN	VALUE	FROM	TO
 Wrapped Ether	2000000000000000	 Palla: simulate test	 0x28ce...e122
 0x1f98...f984	30100360100798670	 0x28ce...e122	 0x07a9...B606


 Wrapped Ether

Events

Deposit, Transfer

Storage

3/3 Slots Changed


 0x1f98...f984

Events

Transfer

Storage

2/2 Slots Changed

 0x28ce...e122

Events

Sync, Swap

Storage

5/5 Slots Changed



What to look for?

## Contracts involved

State changes

Events: transfer, approval, roles, ownership, upgrades, etc

## Simulated Transaction

This is the list of all project and publicly verified contracts that have been involved in this transaction. Select a contract below to view its source.

**Uni**

0x1f9840a8...f984

✓ Verified Contract

**UniswapV2Pair**

0x28cee28a...e122

✓ Verified Contract

**GnosisSafeL2**

0x3e5c6364...d36e

✓ Verified Contract

**UniswapV2Router02**

0x7a250d56...488d

✓ Verified Contract

**WETH9**

0xb4fbf271...08d6

✓ Verified Contract

What to look for?

Contracts involved

## State changes

Events: transfer, approval, roles, ownership, upgrades, etc

## Simulated Transaction



Uniswap ERC20

0x1f9840a85d5af5bf1d1762f925bdaddc4201f984

### Storage

mapping (address => uint96) balances

0x07a93b04a0e019cf70025ff3a84943f695b5b606

0

→

30109535596167258

0x28cee28a7c4b4022ac92685c07d2f33ab1a0e122

2020681068028...

→

2020678057075...



UniswapV2Pair

0x28cee28a7c4b4022ac92685c07d2f33ab1a0e122

### Storage

uint112 reserve0

202068106802865929552...

→

202067805707509967879...

uint112 reserve1

133819136231401819211...

→

133819336231401819211...

uint32 blockTimestampLast

1665091104

→

1665091317

uint256 price0CumulativeLast

239725703211979989663...

→

239726435630921917372...

uint256 price1CumulativeLast

324047077163041742379...

→

324047093863126220297...

What to look for?

Contracts involved

State changes

**Events:** transfer, approval, roles, ownership, upgrades, etc

## Simulated Transaction

SafeMultiSigTransaction



Unknown  
0x07a93b04a0...b5b606

Swap



UniswapV2Pair  
0x28cee28a7c...a0e122

```
{  
  "sender" :  
    "0x7a250d5630b4cf539739df2c5dacb4c659f2488d"  
  "amount0In" : "0"  
  "amount1In" : "200000000000000000"  
  "amount0Out" : "30109535596167258"  
  "amount1Out" : "0"  
  "to" : "0x07a93b04a0e019cf70025ff3a84943f695b5b606"  
}
```

▼ Show raw data and topics

Swap



0x28cee28a7c...a0e122

ExecutionSuccess



Unknown  
0x07a93b04a0...b5b606



Upgrades

# Dealing with contract upgrades

APPROVAL PENDING

## Upgrade to V2

### Description

Upgrades contract to v2.0 with new features.

Vault Goerli contract at address



0x027D19C2e9bb7ab6e5d4341f28dbE60e3CD06029

Network

GOERLI

### Proposed new implementation



0x79839280d18796e715d47f0A9B71C1b7Ac86c2Cd

#### EXECUTION STRATEGY

##### MULTISIG



Team Multisig

2/2 signatures needed

##### CONTRACT



Vault Goerli

upgradeTo

#### TARGET FUNCTION

upgradeTo (



0x7983...c2Cd

)

NEWIMPLEMENTATION: ADDRESS

What does an upgrade tx look like?

**to:** The contract to upgrade

**data:** Upgrade to a new address

#### Interact with:



gor:0x027D19C2e9bb7ab6e5d4341f28dbE60e3CD06029



#### UPGRADE TO

newImplementation(address):

gor:0x79839280...Ac86c2Cd





## Upgraded



Unknown

0x027d19c2e9...d06029

```
{  
  "implementation" :  
  "0x79839280d18796e715d47f0a9b71c1b7ac86c2cd"  
}
```



## Address

0x027d19c2e9bb7ab6e5d4341f28dbe60e3cd06029

## Storage

^ Hide raw state changes

Key: 0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc

Before: 0x000000000000000000000000bde827dc4cb412fa387d914050c4feeb449fc092

After: 0x000000000000000000000000079839280d18796e715d47f0a9b71c1b7ac86c2cd

## PROPOSAL SIMULATION RESULT

Block #7,729,623 - 7 October 2022, 17:19 pm (-03:00)



Vault Goerli

Event

Upgraded

Args

implementatio...



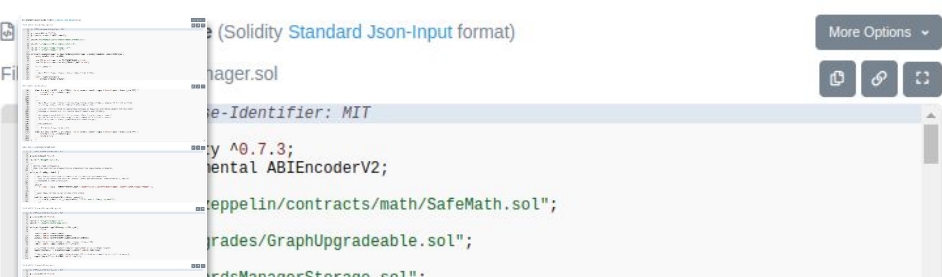
0x7983...c2Cd

What does an upgrade tx look like?

**to:** The contract to upgrade

**data:** Upgrade to a new address



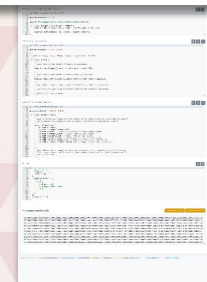


```
(Solidity Standard Json-Input format)
manager.sol
...
Identifier: MIT
...
^0.7.3;
...
ABIEncoderV2;
...
peppelin/contracts/math/SafeMath.sol";
...
grades/GraphUpgradeable.sol";
...
RewardsManagerStorage.sol";
```

## Scope

We audited [PR528](#) up to [commit fdbc60c1e64450123c142d5710a0ae54f489eb8b](#). We also took the opportunity to review:

- RewardsManager
- IRewardsManager
- RewardsManagerV1Storage
- RewardsManagerV2Storage



Verification is necessary  
but not enough

Etherscan

Sourcify

# From source code to deployment

Source code

Associated to a git commit. What devs and auditors review.

Build artifact

Solidity is compiled into bytecode using hardhat or truffle. Bytecode is affected by compiler version and settings.

Address

Bytecode is deployed to the chain and gets assigned an address. What gets executed.



Recompile and compare  
bytecode

Requires scripting knowledge


```
1  # Checkout audited version of the code
2  git checkout 210b5e829fc1d87375af56843a36640d7028cb21
3  # Compile it
4  yarn hardhat compile
5  # Get the compiled bytecode
6  jq -r '.deployedBytecode' artifacts/../../RewardsManager.json > compiled.txt
7  # Get the deployed bytecode
8  seth code 0x7983...c2Cd > deployed.txt
9  # Compare them
10 diff compiled.txt deployed.txt
```

## Upgrade to 0xE2515f74

### Description

Upgrading box contract to new version deployed at <https://github.com/spalladino/test-hardhat-project/actions/runs/3208251267>


Goerli 0x96F2B948 contract at address

 0x96F2B948d4006d9BaF546Ae507A7f27702128C1

Network

GOERLI

### Proposed new implementation

 0xE2515f744ceE0B9bd4BE8331386f1D1EC8ba9A56

#### ON-CHAIN BYTECODE VERIFICATION STATUS

**EXACT MATCH** Compilation artifact and on-chain bytecode are identical.

#### Compilation artifact reference

The compilation artifact was uploaded by the verifier from this location. Check that the artifact hash matches the SHA256 of compilation artifact bytecode displayed below.

<https://github.com/spalladino/...project/actions/runs/3208251267>

#### SHA256 of compilation artifact bytecode

c9c8cb33179bcb0c16fd6e5b935f9d4a5fd1f76ba5b57e7ba476344b0232ef4d

#### SHA256 of on-chain bytecode

b8192d837b2e14bb306642a861db555e35fc17246793b92228fecdd136bb7e13a

#### Verification date

2 minutes ago

#### Verifier

DUjjiHBsF2FkU5VWtrJCP4nDxbboq5kWC (API key id)

Verify again

# Continuous integration and delivery (CI/CD)

## Compilation and deployment should be auditable



Wrapping up

Let's make multi-sigs really multi

# Demand transparency & auditability

The burden is on the proposer, not the signer







# Thank you!

Santiago Palladino  
palla.eth



@smpalladino