Verify, don’t trust

Being a responsible signer

Santiago Palladino
@smpalladino
Hey, can you sign this...?
Understanding the transaction
What’s in a transaction?

to: who are we calling

data: with what

value: and with how much eth
What’s in a proposal?

to: who are we calling
data: with what
value: and with how much eth
Simulate the transaction
How to simulate a tx?

Tenderly

Defender

Blocknative (API only)
What to look for?

Contracts involved

State changes

Events: transfer, approval, roles, ownership, upgrades, etc
What to look for?

Contracts involved

State changes

Events: transfer, approval, roles, ownership, upgrades, etc
What to look for?

Contracts involved

State changes

Events: transfer, approval, roles, ownership, upgrades, etc
What to look for?

Contracts involved

State changes

Events: transfer, approval, roles, ownership, upgrades, etc
Dealing with contract upgrades
What does an upgrade tx look like?

**to:** The contract to upgrade

**data:** Upgrade to a new address
What does an upgrade tx look like?

to: The contract to upgrade
data: Upgrade to a new address
Verification is necessary but not enough

Etherscan

Sourcify

Scope

We audited PR528 up to commit fdbc60c1e64450123c142d5710a0ae54f489eb8b. We also took the opportunity to review:

- RewardsManager
- IRewardsManager
- RewardsManagerV1Storage
- RewardsManagerV2Storage
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

```bash
# Checkout audited version of the code
git checkout 210b5e829fc1d87375af56843a36640d7028cb21
# Compile it
yarn hardhat compile
# Get the compiled bytecode
jq -r '.deployedBytecode' artifacts/..//RewardsManager.json > compiled.txt
# Get the deployed bytecode
seth code 0x7983...c2Cd > deployed.txt
# Compare them
diff compiled.txt deployed.txt
```
Continuous integration and delivery (CI/CD)

Compilation and deployment should be auditable
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