Ethereum Developers
Tutorials and jobs for Ethereum enthusiasts.

Security and smart contracts

26 July 2017 by Jules Dourlens

As you may know, the Ethereum and more widely blockchain community suffered from a lot of hacks. These major hacks involved million of dollars stolen by exploiting security vulnerability in smart contracts developed by companies. Even the most talented programmers can easily make a mistake with code and when something involves money: a lot of people are here to exploit any vulnerabilities.

Here are two smart contract hacking that happened:

- Analysis of the DAO exploit
- The Parity hack explained

Always remember that it happens and you should always think about security when writing smart contracts or any code that involves manipulating money, or sensitive data.

Here are few advices:

- Always check the input data.
- Keep your contracts as simple and small as possible.
- Keep control and always have a simple and secure way to stop your contract and recover it's holdings.
- Use as much as possible modules to keep codebase tiny and built around simple modules as we covered with our inheritance tutorial.
- Be extremely careful about external contract calls, which may execute malicious code and change control flow.

- Understand that your public functions are public, and may be called maliciously. Your private data is also viewable by anyone.

They are many possible flows in a smart contract such as integers overflow and underflow. Always keep up to date and learn about how your code could be exploited.

Please go and read the smart contracts best practices guide on Github. Also, always stay updated by reading news and following suggested peoples on Twitter.

Share :

Related

Getting data from the internet with Oraclize
28 September 2017
In "Ethereum"

Ethereum smart contracts lifecycle
20 July 2017
In "Non classé"

Inheritance in Solidity
25 July 2017
In "Ethereum"

memo, Solidity
< Inheritance in Solidity
> Getting started with Embark Framework

Leave a Comment

Name *

Email *

Website

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Search ...

Memo

Types in Solidity

Testing your Solidity smart contracts

SafeMath to protect from overflows

Getting data from the internet with Oraclize

Recent Posts

Fork and scalability

An introduction to Plasma

ETHWaterloo hackathon was awesome

How to deploy your Truffle projects

Deploy your Truffle smart contracts to the Live Network

Categories

Blog
Design Patern
Embark Framework
Ethereum
memo
Non classé
Solidity
Truffle
Tutorial

Help us

Donating will help us with hosting and supporting free content creation.

Ethereum:
0xC618b905f7b41c7D53C23474322D7D3297730419

Bitcoin:
38ghd1Pokhk6oxs7t1Vna1PxtAy8A7SXWN

Feed

RSS - Posts

RSS - Comments

Navigation