ICE center@ETH

Smart Contract Security - Securify

Hubert Ritzdorf

Smart Contract Security

- What is a smart contract?

Smart Contract Security

- What is a smart contract?
  - Program running on the blockchain (mostly Ethereum)

Smart Contract Security

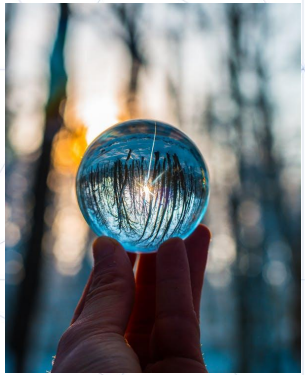
- What is a smart contract?
  - Program running on the blockchain (mostly Ethereum)

- What's special?

Smart Contract Security

- What is a smart contract?
  - Program running on the blockchain (mostly Ethereum)

- What's special?
  - Code and state publicly visible
  - Everyone can interact
  - Handle funds

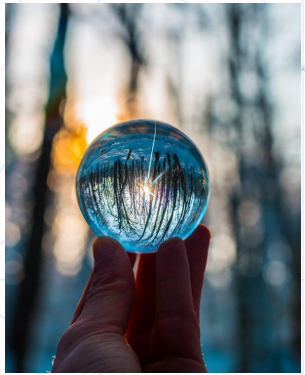


Smart Contract Security

- What is a smart contract?
  - Program running on the blockchain (mostly Ethereum)

- What's special?
  - Code and state publicly visible
  - Everyone can interact
  - Handle funds

- Real Problem?

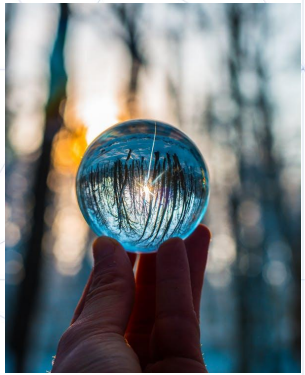


Smart Contract Security

- What is a smart contract?
  - Program running on the blockchain (mostly Ethereum)

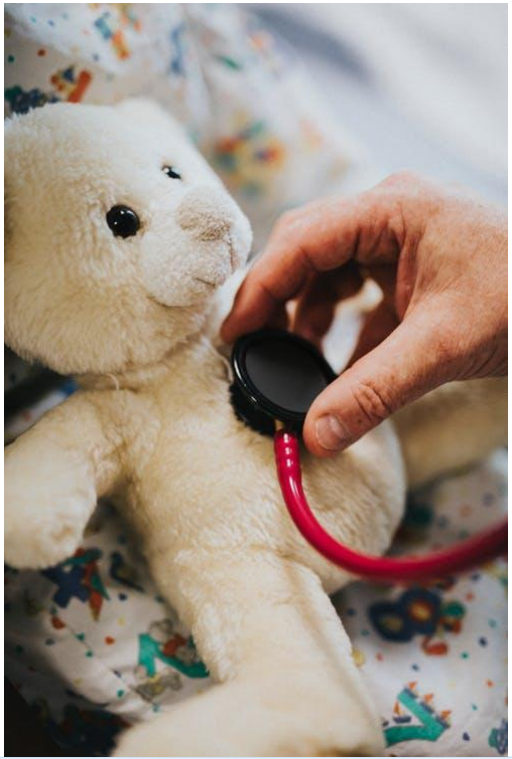
- What's special?
  - Code and state publicly visible
  - Everyone can interact
  - Handle funds

- Real Problem?
  - DAO Hack (2016): caused a hard-fork
  - Parity Multi-Sig Bug (2017): 153,037 ETH (~ 15 million USD)
  - Spankchain Hack (2018): 165.38 ETH (10,000 USD)

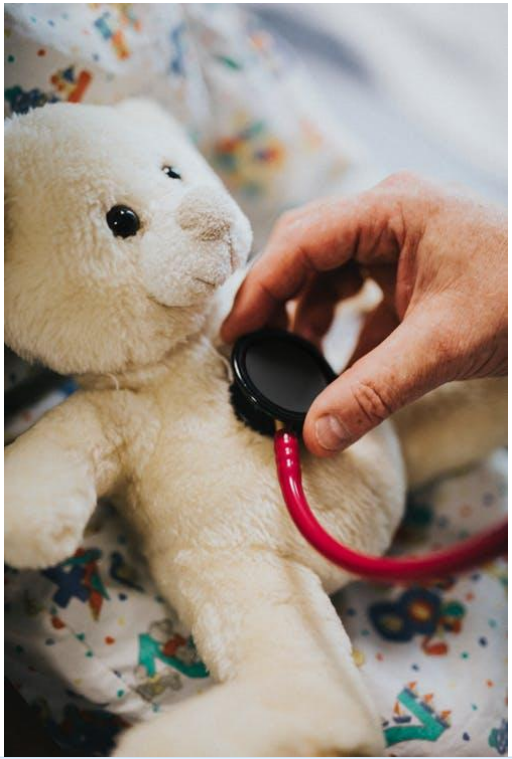


What is Securify? – Simply Explained

What is Securify? – Simply Explained



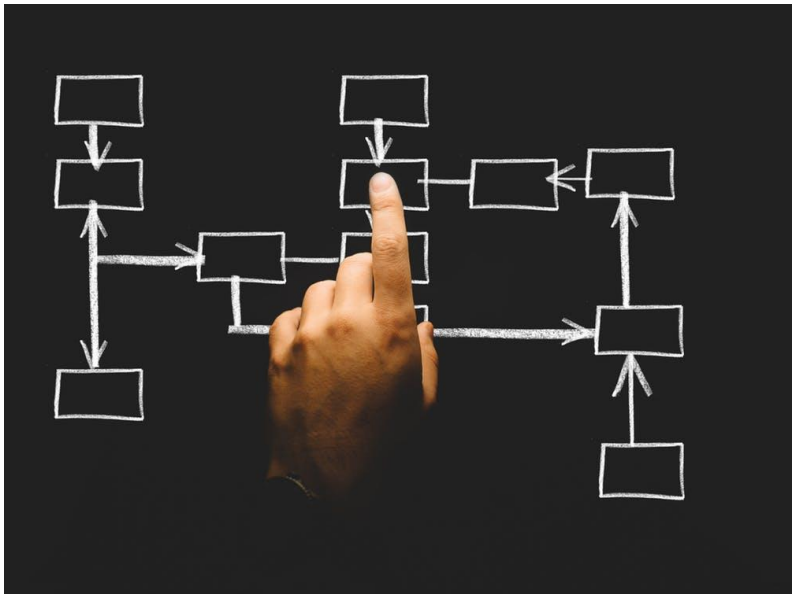
What is Securify? - Simply Explained



- Metasploit for Smart Contracts
- Basic checks

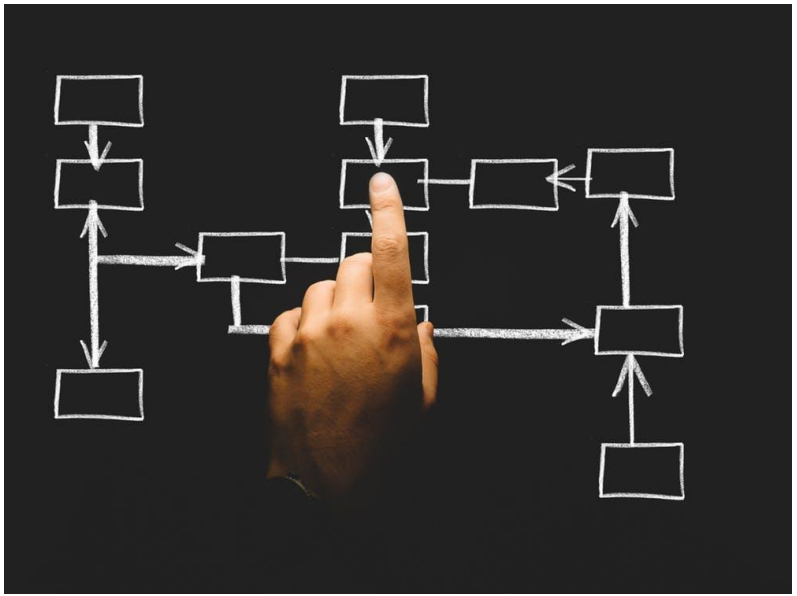
What is Securify? - More complex

What is Securify? - More complex



- Dependency Graph
- Compliances and Violations

What is Securify? - More complex



- Dependency Graph
- Compliances and Violations

- Reentrancy
- Missing authorization
- ...

Try it! https://securify.ch

SCAN NOW | REQUEST AUDIT | PASTE CODE | UPLOAD ZIP | CLONE GIT

```
1  library SafeMath {
2    function add(uint256 a, uint256 b) returns (uint256 c) {
3      c = a + b;
4      assert(c >= a);
5      return c;
6    }
7
8  function mul(uint256 a, uint256 b) internal pure returns (uint256 c) {
9    if (a == 0) {
10     return 0;
11   }
12   c = a * b;
13   assert(c / a == b);
14     return c;
```

Try it!

SCAN NOW | REQUEST AUDIT | PASTE CODE | UPLOAD ZIP | CLONE GIT

```
1  li    SafeMath {
2    f    ion add(uint256 a, uint256 b) returns (uint256 c) {
3          a + b;
4      assert(c >= a);
5      return c;
6    }
7
8  function mul(uint256 a, uint256 b) internal pure returns (uint256 c) {
9    if (a == 0) {
10     return 0;
11   }
12   c = a * b;
13   assert(c / a == b);
14     return c;
```

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

- Academic paper: https://arxiv.org/abs/1806.01143

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

- Academic paper: https://arxiv.org/abs/1806.01143
- Open-source: https://github.com/eth-sri/securify

ethereum foundation grants

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

- Academic paper: https://arxiv.org/abs/1806.01143
- Open-source: https://github.com/eth-sri/securify
- Discord: https://discord.gg/nN77ckb

ethereum foundation grants

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

- Academic paper: https://arxiv.org/abs/1806.01143
- Open-source: https://github.com/eth-sri/securify
- Discord: https://discord.gg/nN77ckb
- Twitter: https://twitter.com/securifyswiss

ethereum foundation grants

Check it out:

https://securify.ch

- Free, One-Click Analysis
- Paste, Upload or Clone

- Academic paper: https://arxiv.org/abs/1806.01143
- Open-source: https://github.com/eth-sri/securify
- Discord: https://discord.gg/nN77ckb
- Twitter: https://twitter.com/securifyswiss

ethereum foundation grants

More coming soon...