Lauro Gripa Neto

Understanding
Ethereum Development

MAGRATHEA LABS

www.magrathealabs.com

SUMMARY

1. Introduction
2. Dependencies
3. Setup
4. DEMO
5. Applications
6. Sources

What is Ethereum?

“Ethereum is a **decentralized platform** that runs **smart contracts:** applications that run exactly as programmed without any possibility of **downtime**, **censorship**, **fraud** or **third-party interference**.” [ethereum.org]

How does Ethereum work?

“(...) apps run on a **custom built blockchain**, an enormously powerful **shared global infrastructure** that can move **value** around and represent the **ownership of property**.” [ethereum.org]

- Smart contracts are written in **Solidity** and deployed as binary codes
- Transactions can be **value transfers** or **contract method calls**
- Code is run by each node using an **EVM** (Ethereum Virtual Machine)
- Therefore, code must be deterministic

Dependencies

- geth 1.7.3-stable
- Solidity v0.4.19
- npm 5.6.0
- node v9.4.0
- Truffle v4.0.6

Running your own node

https://gist.github.com/laurogripa/59d0ea3da3c8b8efac3d8b402ac7a8ae

[DEMO]

Bolacha ou Biscoito?

Limitations

1. Adoption / Regulation
2. Contract language is new (Solidity)
3. Deterministic code and redundancy
4. Scalability
5. Vulnerabilities
    a. Social engineering
    b. Attacks
    c. Bugs

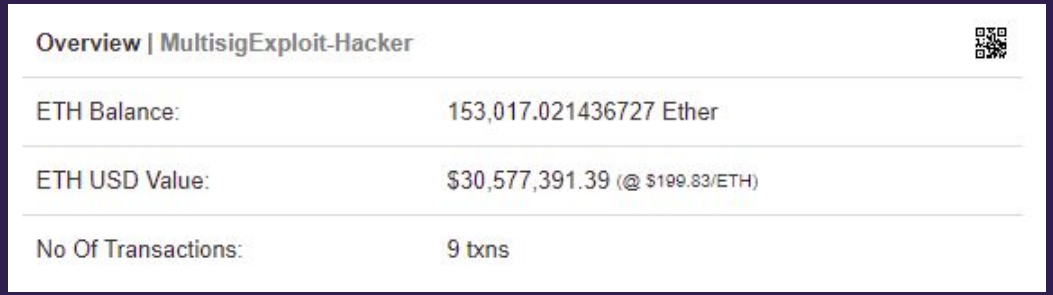
VULNERABILITIES

```
// constructor - just pass on the owner array to the
// multiowned and the limit to daylimit
function initWallet(address[] _owners, uint _required,
uint _daylimit) {
  initDaylimit(_daylimit);
  initMultiowned(_owners, _required);
}
```

VULNERABILITIES

```
function() payable {
  // just being sent some cash?
  if (msg.value > 0)
    Deposit(msg.sender, msg.value);
  else if (msg.data.length > 0)
    _walletLibrary.delegatecall(msg.data);
}
```

EXPLOIT ADDRESS



Overview | MultisigExploit-Hacker	
ETH Balance:	153,017.021436727 Ether
ETH USD Value:	$30,577,391.39 (@ $199.83/ETH)
No Of Transactions:	9 txns

WHITE HAT GROUP

WHITE HAT GROUP ADDRESS

Overview | MultisigExploit-WhiteHat

ETH Balance:	377,113.498729249311671493 Ether
ETH USD Value:	$75,528,291.53 (@ $200.28/ETH)
No Of Transactions:	2558 txns

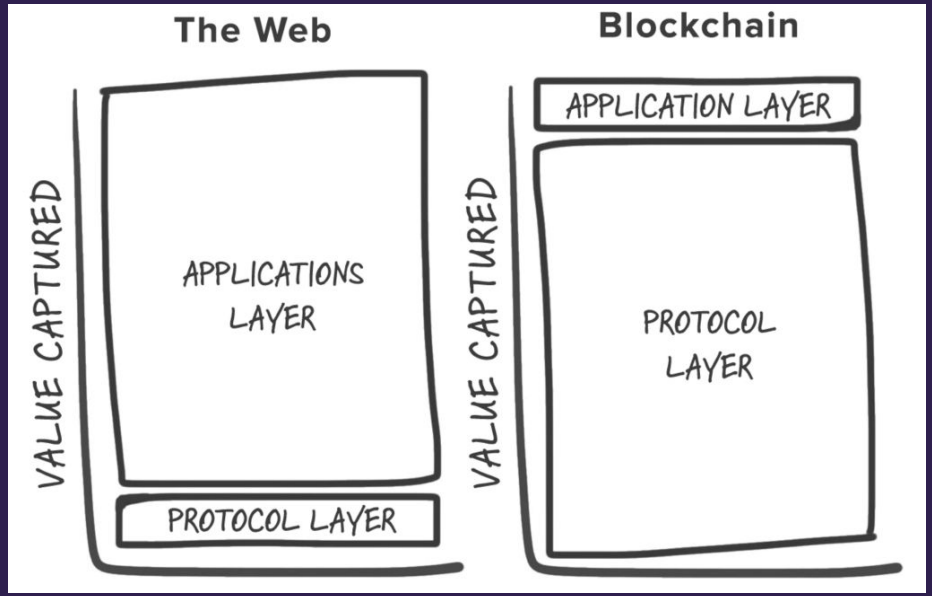
FIXED COMMIT

```
104
105     // constructor is given number of sigs required to do protected "onlymanyowners" transactions
106     // as well as the selection of addresses capable of confirming them.
107 +   function initMultiowned(address[] _owners, uint _required) internal {
108       m_numOwners = _owners.length + 1;
109       m_owners[1] = uint(msg.sender);
110       m_ownerIndex[uint(msg.sender)] = 1;

198     }
199
200     // constructor - stores initial daily limit and records the present day's index.
201 +   function initDaylimit(uint _limit) internal {
202       m_dailyLimit = _limit;
203       m_lastDay = today();
204     }

211       m_spentToday = 0;
212     }
213
214 +   // throw unless the contract is not yet initialized.
215 +   modifier only_uninitialized { if (m_numOwners > 0) throw; _; }
216 +
217     // constructor - just pass on the owner array to the multiowned and
218     // the limit to daylimit
219 +   function initWallet(address[] _owners, uint _required, uint _daylimit) only_uninitialized {
220       initDaylimit(_daylimit);
221       initMultiowned(_owners, _required);
222     }
```

Capturing (and creating) value



The paradox of presales

- 100 million gems will be issued and used to pay for ads
- “Why I don’t use bitcoin instead of gem?”
- However, the token is needed to fund the project

GOLEM

“Golem is a global, open sourced, **decentralized supercomputer that anyone can access**. It's made up of the combined power of user's machines, from personal laptops to entire datacenters.”

source: https://golem.network/

Sources

- https://ethereum.org
- https://medium.com/@mvmurthy/full-stack-hello-world-voting-ethereum-dapp-tutorial-part-1-40d2d0d807c2
- https://medium.com/@mvmurthy/full-stack-hello-world-voting-ethereum-dapp-tutorial-part-2-30b3d335aa1f
- https://gist.github.com/laurogripa/59d0ea3da3c8b8efac3d8b402ac7a8ae
- https://github.com/laurogripa/voting-dapp
- http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html
- http://truffleframework.com
- https://github.com/ethereum/web3.js/
- https://github.com/ethereum/go-ethereum
- https://tpbit.blogspot.com.br/2014/12/the-paradox-of-presales-pondering-gems.html

MAGRATHEA LABS

www.magrathealabs.com
contact@magrathealabs.com

Thank you!

MAGRATHEA LABS

www.magrathealabs.com