Formal Verification in Scala

Ramon Boss, Anna Doukmak

June 7, 2019

Table of Contents

What is The DAO

Majority voting attack

Why there is no new The DAO

Table of Contents

What is The DAO

Majority voting attack

Why there is no new The DAO

What is The DAO

Basics

- Investment fund
- Autonomous
- Voting right based on invested amount

What is The DAO

Basics

- Investment fund
- Autonomous
- Voting right based on invested amount

Technology

- An open-source software
- Written in Solidity
- Build on Ethereum blockchain

Initial Phase

- Defines the contract
- Minimum ETH needed
- Fixed end time

Initial Phase

- Defines the contract
- Minimum ETH needed
- Fixed end time

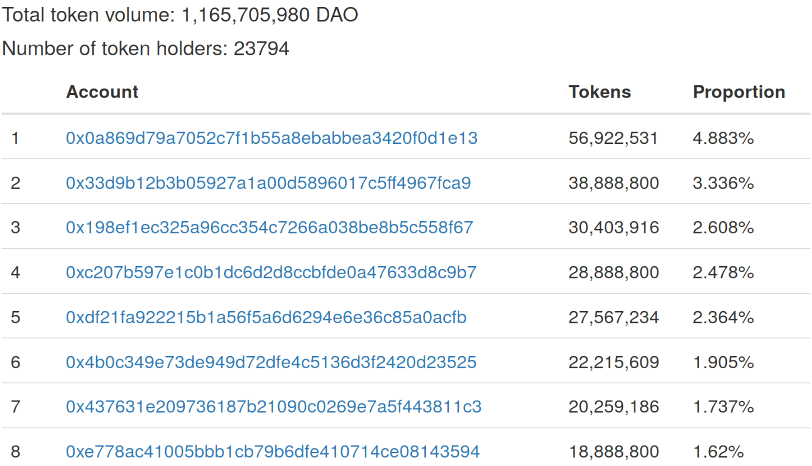
```
contract DAO is DAOInterface {
  uint constant minProposalDebatePeriod = 2 weeks;
  uint public proposalDeposit;
  mapping (address => bool) public allowedRecipients;

  function DAO(uint _proposalDeposit) {
    proposalDeposit = _proposalDeposit;
    allowedRecipients[address(this)] = true;
  }
}
```

Investors

- Invest in The DAO
- A Ethereum wallet address
- Gets DAO tokens
- Receive reward

Example Investors



Total token volume: 1,165,705,980 DAO

Number of token holders: 23794

	Account	Tokens	Proportion
1	0x0a869d79a7052c7f1b55a8ebabbea3420f0d1e13	56,922,531	4.883%
2	0x33d9b12b3b05927a1a00d5896017c5ff4967fca9	38,888,800	3.336%
3	0x198ef1ec325a96cc354c7266a038be8b5c558f67	30,403,916	2.608%
4	0xc207b597e1c0b1dc6d2d8ccbfde0a47633d8c9b7	28,888,800	2.478%
5	0xdf21fa922215b1a56f5a6d6294e6e36c85a0acfb	27,567,234	2.364%
6	0x4b0c349e73de949d72dfe4c5136d3f2420d23525	22,215,609	1.905%
7	0x437631e209736187b21090c0269e7a5f443811c3	20,259,186	1.737%
8	0xe778ac41005bbb1cb79b6dfe410714ce08143594	18,888,800	1.62%

Proposal

- Recipient
- Amount
- Deadline
- Creator

Proposal

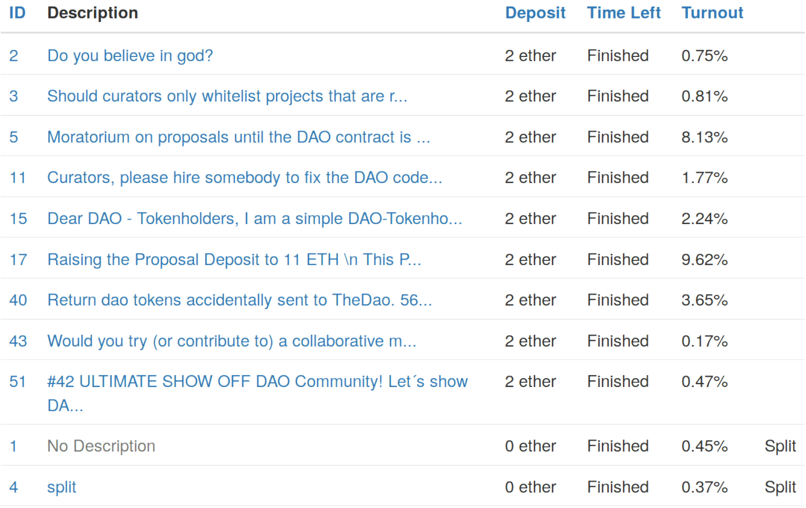
- Recipient
- Amount
- Deadline
- Creator

```
struct Proposal {
  address recipient;
  uint amount;
  string description;
  uint votingDeadline;
  uint proposalDeposit;
  address creator;
}
```

Example Proposal

Mobotiq's vision of modular Electric Vehicles that can be rented P2P is a perfect fit for the blockchain. Integration with Ethereum could enable the development of fully autonomous, self-renting vehicles.

Proposal List



ID	Description	Deposit	Time Left	Turnout	
2	Do you believe in god?	2 ether	Finished	0.75%	
3	Should curators only whitelist projects that are r...	2 ether	Finished	0.81%	
5	Moratorium on proposals until the DAO contract is ...	2 ether	Finished	8.13%	
11	Curators, please hire somebody to fix the DAO code...	2 ether	Finished	1.77%	
15	Dear DAO - Tokenholders, I am a simple DAO-Tokenho...	2 ether	Finished	2.24%	
17	Raising the Proposal Deposit to 11 ETH \n This P...	2 ether	Finished	9.62%	
40	Return dao tokens accidentally sent to TheDao. 56...	2 ether	Finished	3.65%	
43	Would you try (or contribute to) a collaborative m...	2 ether	Finished	0.17%	
51	#42 ULTIMATE SHOW OFF DAO Community! Let´s show DA...	2 ether	Finished	0.47%	
1	No Description	0 ether	Finished	0.45%	Split
4	split	0 ether	Finished	0.37%	Split

Table of Contents

What is The DAO

Majority voting attack

Why there is no new The DAO

Curator

- Controls the whitelist
- Checks proposals

Table of Contents

What is The DAO

Majority voting attack

Why there is no new The DAO

Why there is no new The DAO

- Profitableness
- Law
- Voting problem
- The stalker