



Florian Antony
Phone: +49 (0) 231 9860 219
Email: florian.antony@itemis.de

Agenda



Introduction

What are Smart Contracts, Ethereum and Solidity?

Motivation

Why are we building Tools for Solidity?

Live Demo

How can YAKINDU Solidity Tools help?

Preview

What is planned for the future?

Smart Contracts

Introduction



- ***software that represents a contract***
- ***describes rights and duties of participating parties***
- ***digitally enforces or executes***

Ethereum

Introduction

- ***decentralized platform that runs smart contracts***
Ethereum Virtual Machine (EVM)
- *developed by the **Ethereum Foundation***
- based on ***block chain technology***
- ***cryptocurrencies e.g. Ether(ETH) are smart contracts***



ethereum

Solidity

Introduction



- **programming language to define smart contract**
- **most popular language to run on the EVM**

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public constant returns (uint) {
        return storedData;
    }
}
```



Solidity Features

Motivation



...literally everything:

- *multiple inheritance*
- *extension methods*
- *function overloading*
- *multiple return values*
- *function modifiers*
- *...*

Solidity Tooling

Motivation

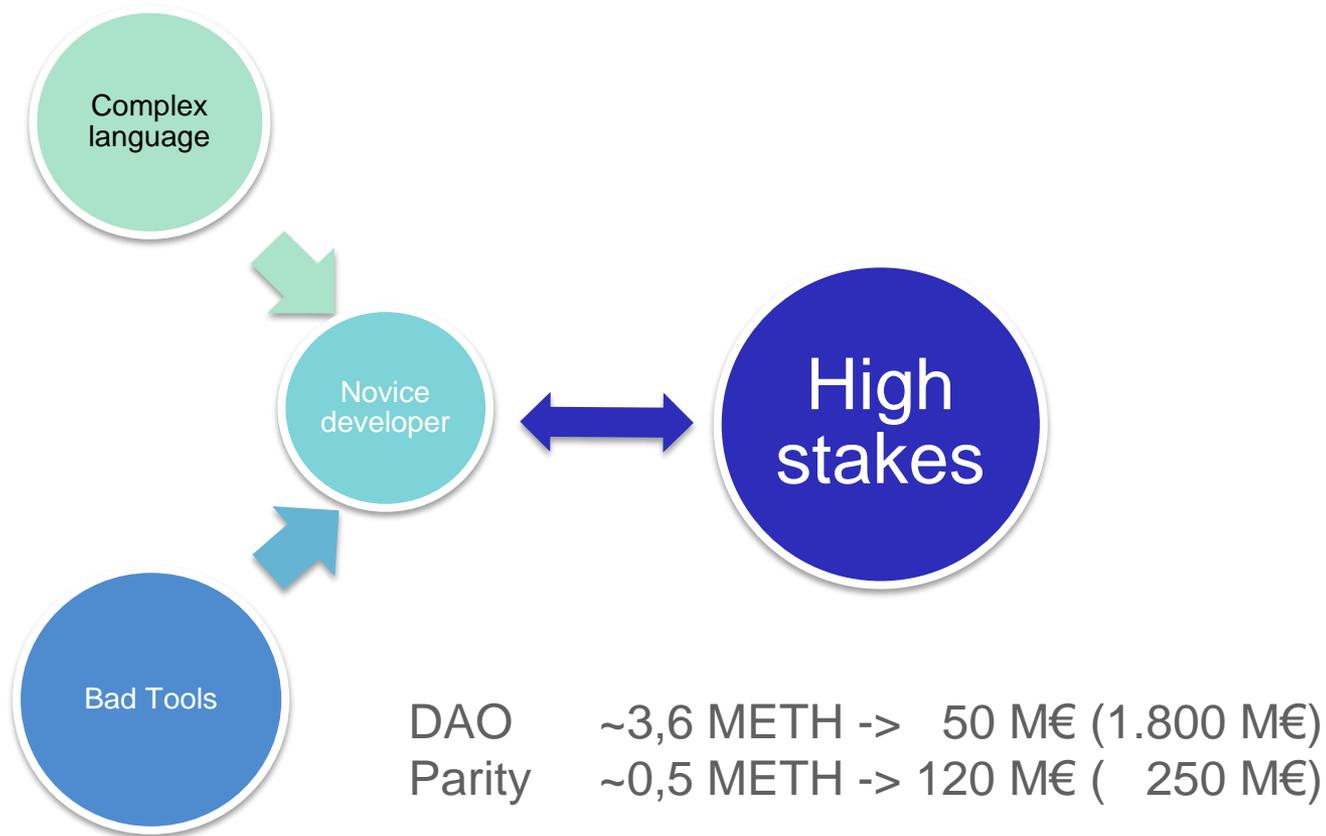


... offers almost nothing:

```
browser/ballot.sol x
10 struct Proposal {
11     uint voteCount;
12 }
13
14 address chairperson;
15 mapping(address => Voter) voters;
16 Proposal[] proposals;
17
18 /// Create a new ballot with $_numProposals) different proposals.
19 function Ballot(uint8 _numProposals) public {
20     chairperson = msg.sender;
21     voters[chairperson] = voters;
22     proposals.length = msg;
23 }
24
25 /// Give $(toVoter) the right to vote.
26 /// May only be called by the chairperson.
27 function giveRightToVote(address toVoter) public {
28     if (msg.sender != chairperson) return;
29     voters[toVoter].weight = 1;
30 }
31
32 /// Delegate your vote to the voter $(to).
33 function delegate(address to) public {
34     Voter storage sender = voters[msg.sender]; // assigns reference
35     if (sender.voted) return;
36     while (voters[to].delegate != address(0) && voters[to].delegate != msg.sender)
37         to = voters[to].delegate;
38     if (to == msg.sender) return;
39     sender.voted = true;
40     sender.delegate = to;
```

What could possibly go wrong?

Motivation



YAKINDU Solidity IDE

Demo



Features

- ***meaningful code completion***
- ***quick fixes***
- ***code navigation***
- ***code formatting***
- ***syntax highlighting***
- ***templates***
- ***...***





Live Demo I



```
// This is a type for a single proposal.
struct Proposal{
    bytes32 name; // short name (up to 32 bytes)
    uint voteCount; // number of accumulated votes
}

address public chairperson;
// This declares a state variable that
// stores a `Voter` struct for each possible address.
mapping(address => Voter) public voters;
// A dynamically-sized array of `Proposal` structs.
Proposal[] public proposals;

// // Create a new ballot to choose one of `proposalNames`.
function Ballot(bytes32[] proposalNames) public{
    chairperson = msg.sender;
    voters[chairperson]
    // For each of the
    // create a new pro
    // to the end of th
    for (uint i = 0;
        i < proposalNames.l
```

Special Variables and Functions

There are special variables and functions which always exist in the global namespace and are mainly used to provide information about the blockchain.

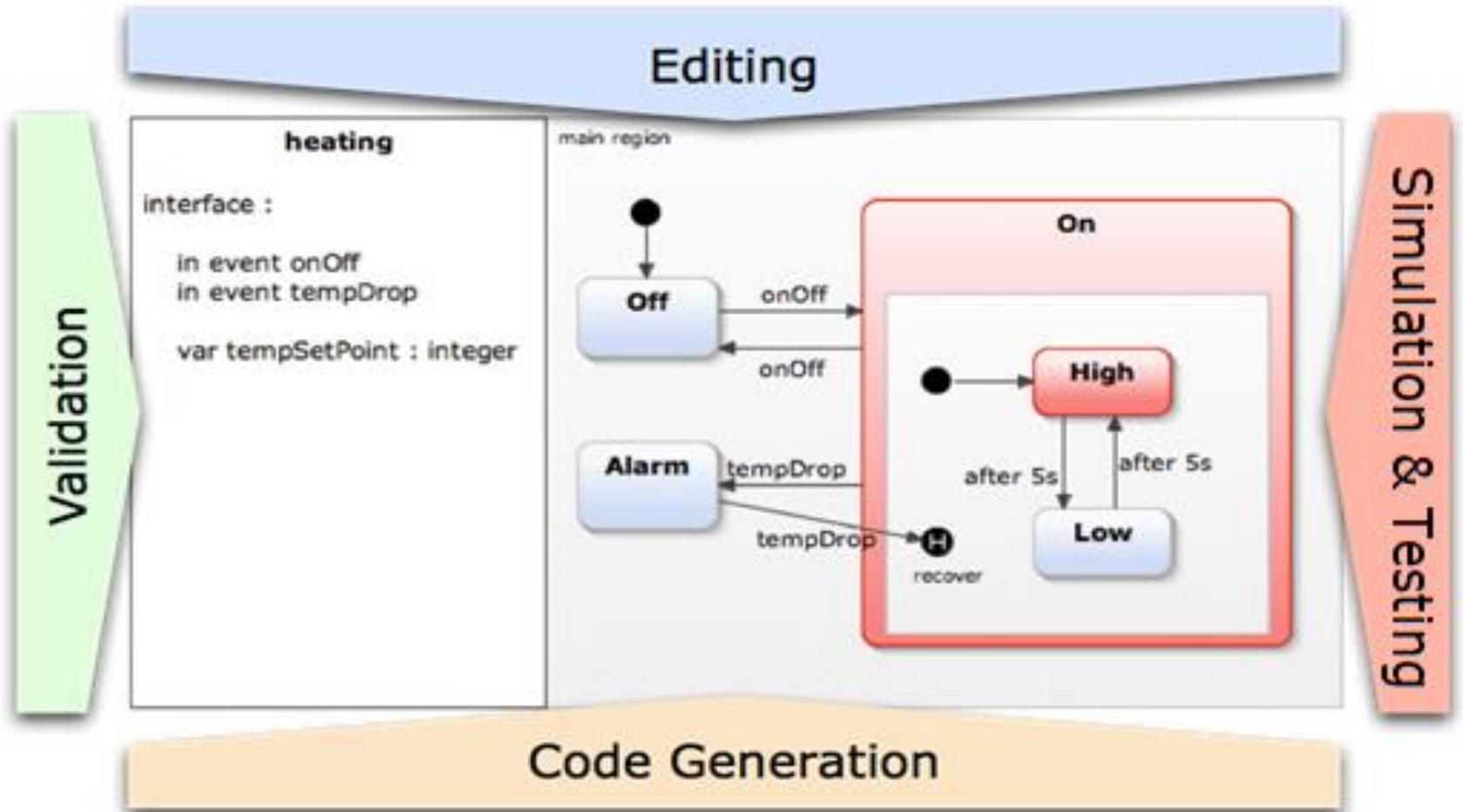
Block and Transaction Properties

- `block.blockhash(uint blockNumber)` returns (bytes32): hash of the given block - only works for 256 most recent blocks excluding current
- `block.coinbase(address)`: current block miner's address
- `block.difficulty(uint)`: current block difficulty

Description	File	Line	Message
Warning: This declaration shadows an existing declaration	my_contract.... /Test/src	line: 115 /Test/...	Xtext Check (...)
Warning: This declaration shadows an existing declaration	my_contract.... /Test/src	line: 131 /Test/...	Xtext Check (...)
Warning: This declaration shadows an existing declaration	my_contract.... /Test/src	line: 87 /Test/...	Xtext Check (...)
Info: Gas estimations:	my_contract.... /Test/src	line: 1 /Test/s...	Xtext Check (...)

YAKINDU Statechart Tools

Demo





@yakindu



<https://github.com/Yakindu/solidity-ide>





Contact in Switzerland:

Serano Colameo

Phone: +41 (0)56 442 68 63

Email: serano.colameo@itemis-schweiz.ch

itemis Schweiz GmbH | Dorfstrasse 69 | CH-5210 Windisch | www.itemis-schweiz.ch

