# A living programming environment for a living blockchain



by Santiago Bragagnolo - PharoDays - 2017 santiago.bragagnolo@gmail.com santiago.bragagnolo@inria.fr skype:santiago.bragagnolo @sbragagnolo





## Disclaimer!

#### This is not a blockchain mechanisms talk! (Sorry disappoint you :))



## General technology explanation



### Starting by the fruit: Smart contracts

- Digital reification of contracts
  - Emulate the logic of contractual clauses
  - Self-executing
  - Self-enforcing
- Reduce transactional costs
- Minimise exceptions





# Following by the branch: Ethereum

- Blockchain based technology
- Open source & public network
- Smart contracts
  - State stored in a blockchain
  - Byte-code executed in the turing complete EVM
  - Many development languages (solidity, serpent, etc)





#### Arriving to the trunk: Blockchain

- Open and distributed ledger
- Records a constantly-growing list of transactions in between two parties. (blocks)
- Resistant to modification by design
- Cryptocurrency: Paying to reinforce the social engagement with the security





## First-citizens in Blockchain

- Block: stamped batch of transactions
- Transaction: Representation of mutations of state
  - Movements of money
  - Method activation
- Account: Source and target of transactions (account in the accountancy meaning)
- Contracts (Specific in ethereum)





# So what? Architecture of a proposed application



## Pharo



## Pharo: Why?

- Blockchain is a multiple actors always growing environment.
- Blockchain is a living environment
  - Transactions move money (ether bitcoin) from one place to other
  - Transactions execute smart contracts
- Ethereum is a distributed runtime. Nothing better than a live environment for a living distributed runtime.
- A lot of code analysis and inspection state-of-the-art tools





Fog

- Pharo client for the Ethereum client (GEth)
- github.com/sbragagnolo/Fog





# Fog - features

- Connection, communication, marshalling, etc.
- Block fetching
- Query and create transactions
- Query and create contracts
- Remote method invocation





# Fog - features

- Development support
  - First-class citizen navigation (GT-Tools)
    - Accounts
    - Blocks
    - Transactions
    - Contracts
  - Automatic contract mirror generation
  - Automatic contract proxy building





## Fog - features

- Cache
  - General
  - Connection
  - Session



## Some fancy slides :)



# Block inspection

- Navigating blocks
- Inspecting blocks individually
- Overview of a collection of blocks through statistics
- Overview of the transactions of a collection of blocks





#### Navigating in blocks

Nation         Value           ( ) self         an Array (10240 items) (Elock- 0 Created 17192:14:56:53.401614 ago 7 trasset)           ( ) self         an Array (10240 items) (Elock- 0 Created 17192:14:56:53.401614 ago 7 trasset)           ( ) self         an Array (10240 items) (Elock- 0 Created 17192:14:56:53.520614 ago 7 transaction(s) '           ( ) self         an Array (10240 items) (Elock- 0 Created 17192:14:56:53.520614 ago 7 transaction(s) '           ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	A Stats	Block View R	Raw Meta		0.00	1 50
Value         Value           () self         an Array [10240 items] ('Block- 0 Created 17192:14:56:53.401614 ago 7 transaction(s)'           () 1         'Block- 0 Created 17192:14:56:53.522614 ago 7 transaction(s)'           () 2         'Block- 0 Created 17192:14:56:53.522614 ago 7 transaction(s)'           () 3         'Block- 0 Created 17192:14:56:53.527671 ago 8 transaction(s)'           () 6 3         'Block- 0 Created 17192:14:56:53.539601 ago 8 transaction(s)'           () 6 4         'Block- 0 Created 17192:14:56:53.537485 ago 8 transaction(s)'           () 6 5         'Block- 0 Created 17192:14:56:53.59137 ago 1 transaction(s)'           () 6 8         'Block- 0 Created 17192:14:56:53.59137 ago 1 transaction(s)'           () 6 8         'Block- 0 Created 17192:14:56:53.597088 ago 1 transaction(s)'           () 6 9         'Block- 0 Created 17192:14:56:53.597617 ago 1 transaction(s)'           () 6 9         'Block- 0 Created 17192:14:56:53.597617 ago 1 transaction(s)'           () 7         'Block- 0 Created 17192:14:56:53.69677 ago 7 transaction(s)'           () 7         'Block- 0 Created 17192:14:56:53.697659 ago 7 transaction(s)'           () 7         'Block- 0 Created 17192:14:56:53.697659 ago 7 transaction(s)'           () 8         'Block- 0 Created 17192:14:56:53.915439 ago 6           () 7         'Block- 0 Created 17192:14:56:53.915439 ago 6           () 7         'Block- 0	A				~ ~ ~	1 👓
<pre>() self an Array [10240 items] ('Elock- 0 Created 17192:14:56:53.491614 ago 7 trans () 1 'Block- 0 Created 17192:14:56:53.520614 ago 7 transaction(s)' () 2 'Block- 0 Created 17192:14:56:53.527671 ago 8 transaction(s)' () 3 'Block- 0 Created 17192:14:56:53.539601 ago 8 transaction(s)' () 4 'Block- 0 Created 17192:14:56:53.539601 ago 9 transaction(s)' () 5 'Block- 0 Created 17192:14:56:53.543794 ago 0 transaction(s)' () 6 'Block- 0 Created 17192:14:56:53.543794 ago 0 transaction(s)' () 6 'Block- 0 Created 17192:14:56:53.57488 ago 8 transaction(s)' () 6 'Block- 0 Created 17192:14:56:53.571782 ago 1 transaction(s)' () 7 'Block- 0 Created 17192:14:56:53.570088 ago 1 transaction(s)' () 8 'Block- 0 Created 17192:14:56:53.570088 ago 1 transaction(s)' () 9 'Block- 0 Created 17192:14:56:53.50577 ago 0 transaction(s)' () 11 'Block- 0 Created 17192:14:56:53.605077 ago 1 transaction(s)' () 11 'Block- 0 Created 17192:14:56:53.605077 ago 1 transaction(s)' () 12 'Block- 0 Created 17192:14:56:53.6020486 ago 0 transaction(s)' () 13 'Block- 0 Created 17192:14:56:53.6020486 ago 0 transaction(s)' () 14 'Block- 0 Created 17192:14:56:53.6020486 ago 0 transaction(s)' () 2) 20 Created 17192:14:56:53.9154389 ago 0 Create</pre>						
• © 1       'Block-0 Created 17192:14:56:53.522614 ago 7 transaction(s)'         • © 2       'Block-0 Created 17192:14:56:53.527671 ago 8 transaction(s)'         • © 3       'Block-0 Created 17192:14:56:53.339601 ago 8 transaction(s)'         • © 4       'Block-0 Created 17192:14:56:53.537485 ago 8 transaction(s)'         • © 5       'Block-0 Created 17192:14:56:53.547485 ago 1 transaction(s)'         • © 6       'Block-0 Created 17192:14:56:53.57782 ago 1 transaction(s)'         • © 7       'Block-0 Created 17192:14:56:53.57782 ago 1 transaction(s)'         • © 6       'Block-0 Created 17192:14:56:53.577088 ago 1 transaction(s)'         • © 7       'Block-0 Created 17192:14:56:53.57068 ago 1 transaction(s)'         • © 8       'Block-0 Created 17192:14:56:53.59517 ago 1 transaction(s)'         • © 9       'Block-0 Created 17192:14:56:53.69677 ago 1 transaction(s)'         • © 10       'Block-0 Created 17192:14:56:53.69677 ago 1 transaction(s)'         • © 11       'Block-0 Created 17192:14:56:53.69677 ago 1 transaction(s)'         • © 12       'Block-0 Created 17192:14:56:53.69677 ago 1 transaction(s)'         • © 13       'Block-0 Created 17192:14:56:53.697859 ago 7 transaction(s)'         • * Block-0 Created 17192:14:56:53.915439 ago 0       ''''''''''''''''''''''''''''''''''''						
► © 2 'Block-0 Created 17192:14:56:53.527671 ago 3 transaction(s)' ► © 3 'Block-0 Created 17192:14:56:53.543794 ago 0 transaction(s)' ► © 4 'Block-0 Created 17192:14:56:53.543794 ago 0 transaction(s)' ► © 5 'Block-0 Created 17192:14:56:53.543794 ago 1 transaction(s)' ► © 6 'Block-0 Created 17192:14:56:53.517782 ago 1 transaction(s)' ► © 7 'Block-0 Created 17192:14:56:53.571782 ago 1 transaction(s)' ► © 8 'Block-0 Created 17192:14:56:53.571782 ago 1 transaction(s)' ► © 9 'Block-0 Created 17192:14:56:53.57617 ago 0 transaction(s)' ► © 10 'Block-0 Created 17192:14:56:53.507617 ago 0 transaction(s)' ► © 10 'Block-0 Created 17192:14:56:53.609677 ago 1 transaction(s)' ► © 11 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ► © 12 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ► © 13 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ► © 14 'Block-0 Created 17192:14:56:53.609769 ago 7 transaction(s)' ■ a Array('Block- 0 Created 17192:14:56:53.807659 ago 7 transaction(s) ' ■ a Array('Block- 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block- 0 Created 17192:1etc*		'Block-	0 Created 1	17192:14:58:11.400115 ago 7 transactior	n(s)'	
▶ © 3 'Block-0 Created 17192:14:56:53.539601 ago 3 transaction(s)' > © 4 'Block-0 Created 17192:14:56:53.543794 ago 0 transaction(s)' > © 5 'Block-0 Created 17192:14:56:53.507485 ago 3 transaction(s)' > © 6 'Block-0 Created 17192:14:56:53.571782 ago 1 transaction(s)' > © 7 'Block-0 Created 17192:14:56:53.57068 ago 1 transaction(s)' > © 8 'Block-0 Created 17192:14:56:53.579088 ago 1 transaction(s)' > © 9 'Block-0 Created 17192:14:56:53.579088 ago 1 transaction(s)' > © 9 'Block-0 Created 17192:14:56:53.567617 ago 0 transaction(s)' > © 10 'Block-0 Created 17192:14:56:53.669677 ago 1 transaction(s)' > © 11 'Block-0 Created 17192:14:56:53.609677 ago 1 transaction(s)' > © 12 'Block-0 Created 17192:14:56:53.620486 ago 0 transaction(s)' > © 13 'Block-0 Created 17192:14:56:53.620486 ago 0 transaction(s)' > © 14 'Block-0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' "an Array('Block-0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' "an Array('Block-0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' B Created 17192:14: 'Block-0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block-0 Created 17192:11etc" self		transactions -	> '7 transactio	on(s) AVG gast0 AVG gas-price:0 AVG ether:0'		-
► © 4 'Block 0 Created 17192:14:56:53.543/94 ago 0 transaction(s)' Block 0 Created 17192:14:56:53.557488 ago 3 transaction(s)' Block 0 Created 17192:14:56:53.557488 ago 1 transaction(s)' Block 0 Created 17192:14:56:53.571782 ago 1 transaction(s)' C 6 'Block 0 Created 17192:14:56:53.571782 ago 1 transaction(s)' C 6 'Block 0 Created 17192:14:56:53.571782 ago 1 transaction(s)' C 6 'Block 0 Created 17192:14:56:53.57088 ago 1 transaction(s)' C 9 'Block 0 Created 17192:14:56:53.567617 ago 0 transaction(s)' C 9 'Block 0 Created 17192:14:56:53.56377 ago 1 transaction(s)' C 10 'Block 0 Created 17192:14:56:53.609677 ago 1 transaction(s)' C 11 'Block 0 Created 17192:14:56:53.609677 ago 1 transaction(s)' C 12 'Block 0 Created 17192:14:56:53.609677 ago 1 transaction(s)' C 13 'Block 0 Created 17192:14:56:53.60486 ago 0 transaction(s)' C 14 'Block 0 Created 17192:14:56:53.60486 ago 1 transaction(s)' C 14 'Block 0 Created 17192:14:56:53.60486 ago 0 transaction(s)' C 14 'Block 0 Created 17192:14:56:53.607659 ago 7 transaction(s) ' 'Block 8 Created 17192:14: 'Block 8 Created 17192:14:56:53.915439 ago 6 transaction(s) ' 'Block 8 Created 17192:1etc' self		parent->'Bloo	ck- 0 Created	17192:14:58:11.405058 ago 0 transaction(s) '		
► © 5 'Block 0 Created 17192:14:56:53.557485 ago 3 transaction(s)' E © 6 'Block 0 Created 17192:14:56:53.56137 ago 1 transaction(s)' E © 7 'Block 0 Created 17192:14:56:53.571782 ago 1 transaction(s)' E © 8 'Block 0 Created 17192:14:56:53.570088 ago 1 transaction(s)' E © 9 'Block 0 Created 17192:14:56:53.567617 ago 0 transaction(s)' E © 10 'Block 0 Created 17192:14:56:53.5637 ago 1 transaction(s)' E © 10 'Block 0 Created 17192:14:56:53.606677 ago 7 transaction(s)' E © 11 'Block 0 Created 17192:14:56:53.606677 ago 7 transaction(s)' E © 12 'Block 0 Created 17192:14:56:53.606677 ago 7 transaction(s)' E © 13 'Block 0 Created 17192:14:56:53.620486 ago 0 transaction(s)' E © 14 'Block 0 Created 17192:14:56:53.626449 ago 5 transaction(s)' "an Array('Block + 0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' 'Block 8 Created 17192:14: 'Block - 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block - 0 Creat		uncles -> '0 ite	em(s)'			
<ul> <li>C 6</li> <li>'Block 0 Created 17192:14:56:53.50137 ago 1 transaction(s)'</li> <li>C 7</li> <li>'Block 0 Created 17192:14:56:53.571088 ago 1 transaction(s)'</li> <li>C 8</li> <li>'Block 0 Created 17192:14:56:53.507617 ago 0 transaction(s)'</li> <li>C 9</li> <li>'Block 0 Created 17192:14:56:53.50337 ago 1 transaction(s)'</li> <li>C 10</li> <li>'Block 0 Created 17192:14:56:53.50337 ago 1 transaction(s)'</li> <li>C 11</li> <li>'Block 0 Created 17192:14:56:53.609677 ago 7 transaction(s)'</li> <li>C 11</li> <li>'Block 0 Created 17192:14:56:53.609677 ago 7 transaction(s)'</li> <li>C 12</li> <li>'Block 0 Created 17192:14:56:53.620486 ago 0 transaction(s)'</li> <li>C 13</li> <li>'Block 0 Created 17192:14:56:53.620486 ago 0 transaction(s)'</li> <li>C 14</li> <li>'Block 0 Created 17192:14:56:53.620489 ago 5 transaction(s)'</li> <li>'Block 0 Created 17192:14:56:53.820499 ago 5 transaction(s)'</li> <li>'Block 0 Created 17192:14:56:53.820499 ago 5 transaction(s)'</li> <li>'Block 0 Created 17192:14:56:53.820499 ago 6 transaction(s)'</li> <li>'Block 0 Created 17192:14:56:53.915439 ago 0</li> <li>transaction(s) '''Block-0 Created 17192:1etc''</li> </ul>		hash -> '0x025	fa3d7601cc0a	a3a9296541c62cc09f1a689bdf598debe85da3e823	3796efb6d	1
▶ © 7 'Block-0 Created 17192:14:56:53.571782 ago 1 transaction(s)' ■ © 8 'Block-0 Created 17192:14:56:53.57068 ago 1 transaction(s)' ■ © 9 'Block-0 Created 17192:14:56:53.507617 ago 0 transaction(s)' ■ © 10 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ■ © 11 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ■ © 12 'Block-0 Created 17192:14:56:53.609677 ago 0 transaction(s)' ■ © 13 'Block-0 Created 17192:14:56:53.620486 ago 0 transaction(s)' ■ © 14 'Block-0 Created 17192:14:56:53.628449 ago 5 transaction(s)' "an Array('Block- 0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' 'Block- 0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' 'Block- 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block- 0 Created 17192:1etc"						_
▶ © 8 'Block-0 Created 17192:14:56:53.579088 ago 1 transaction(s)' ■ © 9 'Block-0 Created 17192:14:56:53.567617 ago 0 transaction(s)' ■ © 10 'Block-0 Created 17192:14:56:53.69677 ago 1 transaction(s)' ■ © 11 'Block-0 Created 17192:14:56:53.69677 ago 7 transaction(s)' ■ © 12 'Block-0 Created 17192:14:56:53.690486 ago 0 transaction(s)' ■ © 13 'Block-0 Created 17192:14:56:53.692486 ago 0 transaction(s)' ■ © 14 'Block-0 Created 17192:14:56:53.697659 ago 7 transaction(s)' "an Array('Block-0 Created 17192:14:56:53.697659 ago 7 transaction(s) ' 'Block- 8 Created 17192:14: 'Block- 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block- 0 Created 17192:1etc" self						
▶ © 9 'Block-0 Created 17192:14:56:53.507617 ago 0 transaction(s)' ▷ © 10 'Block-0 Created 17192:14:56:53.50537 ago 1 transaction(s)' ▷ © 11 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ▷ © 12 'Block-0 Created 17197:14:56:53.613171 ago 0 transaction(s)' ▷ © 13 'Block-0 Created 17197:14:56:53.620486 ago 0 transaction(s)' ▷ © 14 'Block-0 Created 17197:14:56:53.620486 ago 5 transaction(s)' "an Array('Block-0 Created 17192:14:56:53.697659 ago 7 transaction(s) ' 'Block- ⊕ Created 17192:14: 'Block- ⊕ Created 17197:14:56:53.915439 ago ⊕ transaction(s) ' 'Block- ⊕ Created 17192:1etc" self						
▶ © 10 'Block-0 Created 17192:14:56:53.50537 ago 1 transaction(s)' ▶ © 11 'Block-0 Created 17192:14:56:53.609677 ago 7 transaction(s)' ▶ © 12 'Block-0 Created 17192:14:56:53.613171 ago 0 transaction(s)' ▶ © 13 'Block-0 Created 17192:14:56:53.620486 ago 0 transaction(s)' ▶ © 14 'Block-0 Created 17192:14:56:53.628449 ago 5 transaction(s)' "an Array('Block-0 Created 17192:14:56:53.607659 ago 7 transaction(s) ' 'Block-0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block-0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block-0 Created 17192:1etc"						
► © 11 'Block-0 Created 17192:14:56:53.606677 ago 7 transaction(s)' ► © 12 'Block-0 Created 17197:14:56:53.613171 ago 0 transaction(s)' ► © 13 'Block-0 Created 17197:14:56:53.620486 ago 0 transaction(s)' ► © 14 'Block-0 Created 17197:14:56:53.628449 ago 5 transaction(s)' "an Array('Block-0 Created 17192:14:56:53.697659 ago 7 transaction(s) ' 'Block-0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block-0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block-0 Created 17192:1etc"						
<pre>&gt; © 12</pre>						
<pre>F @ 13</pre>						
▶ ⓒ 14 'Block-0 Created 17192:14:56:53.628449 ago 5 transaction(s)' "an Array('Block- 0 Created 17192:14:56:53.697659 ago 7 transaction(s) ' 'Block- 8 Created 17192:14: 'Block- 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block- 0 Created 17192:1etc" self						
<pre>"an Array('Block- 0 Created 17192:14:56:53.897659 ago 7 transaction(s) ' 'Block 8 Created 17192:14: 'Block- 0 Created 17192:14:56:53.915439 ago 0 transaction(s) ' 'Block- 0 Created 17192:1etc" self</pre>	w.					





#### Blocks overview







#### Transactions overview







#### Contract source code

pragma solidity ^0.4.2; contract StructTestContract { **enum** myenum { A, B, C } struct mystruct { **bool** boolean; **myenum** uservalue; **uint32** commonvalue; address \_owner; **bool** bool1; **int16** midint; **mystruct** simpleExample; **bool** bool2; mystruct[] arrayExample; function StructTestContract (){ \_owner = msg.sender; bool1 = true;bool2 = true;midint = 32; simpleExample.boolean = true; simpleExample.uservalue = myenum.B; simpleExample.commonvalue = 6355432; arrayExample.push(mystruct(true, myenum.A, 134)); arrayExample.push(mystruct(false, myenum.B, 235)); arrayExample.push(mystruct(true, myenum.C, 34)); function kill() { suicide(\_owner);





#### Inspecting contract

× - 🗆					Inspector on an ETHContractInstanceBind										
an ETHContractInstanceBind			d					<b>&gt;</b>							
B	lock	View	Inspector	Raw	Meta										
	Name				V	/alue									
1	own	er'			<b>'0</b>	xb4ebf466889c4a0239379125a7d0f9c4e8bf2a14'									
1	bool1				tri	ue									
1	midin	ť'			32	2									
'	simple	eExamp	ole"		al	a Dictionary [3 items] ('boolean'->true 'commonvalue'->6355432 'uservalue'->'B' )									
1	bool2				tri	ue									
'	'arrayExample' 'an array of 3 elements '														
	Quick	selectio	on field. Give	n your	INPUT,	, it executes: self select: [:each   INPUT ]									





#### Inspecting structs

× - 🗆	Inspector on an ETHCont	itractInstanceBind								•
an ETHContractInstanceBind		a Dictionary [3 items] ('boolean'->true 'commonvalue'->6355432 'user							D	0,
Block View Inspector Raw Me	ta	It	tems	Keys Ra	w	Meta				
Name	Value		Ксу		Value					
'_owner'	'0xb4ebf466889c4a0239379125a7d0f9c4e8t	1	'boolea	n'	true					
'bool1'	true	1	'userva	ue'			'B'			
'midint'	32	'0	'commo	6355432						
'simpleExample'	a Dictionary [3 items] ('boolean'->true 'com									
'bool2'	true									
'arrayExample'	'an array of 3 elements '									
Quick selection field. Given your INP	UT, it executes: self select: [:each   INPUT ]	(	Quicks	election fi	ield.	Given your INP	UT, it executes: self select: [:each   ]	INPU	IT]	
-										
	8									





## Yet to implement

× –  Inspector on an ETHCor								tractInst	anceBir	ç	5 ? <del>-</del>				
an ETHO	Contract	nstanceBin	d				D	a ByteSt	ring (' an	n array (	of 3 elements ')	x			D) Q
Block	View	Inspector	r Raw Meta						Items	Raw	Meta				
Block View Inspector Raw Meta   Name Value   '_owner' '0xb4ebf466889c4a0239379125a7d0f9c4e8l   'bool1' true   'midint' 32   'simpleExample' a Dictionary [3 items] ('boolean'->true 'com   'bool2' true   'arrayExample' 'an array of 3 elements '							an arr	ay of 3 e	lement	2					
Quick selection field. Given your INPUT, it executes: self select: [:each   INPUT ]															
							0								





# Fog - Demo





# Fog - future

- Finishing session management
- Events support
- Transactional message send recognition
- New AST Definition (Henrique Rocha)





## THANKS :)!

by Santiago Bragagnolo - PharoDays - 2017 <u>santiago.bragagnolo@gmail.com</u> santiago.bragagnolo@inria.fr <u>skype:santiago.bragagnolo</u> @sbragagnolo