Ayana
Consulting

An Introduction to Blockchain and Ethereum

Hands-on

By Marc Lijour

December 12, 2018

The Art and Science of Eternal Blossom

Who am I?

https://www.linkedin.com/in/marclijour/

COLLIDER·X

CONSENSYS

Access these slides

https://bit.ly/2rvX2HJ

or find by date:

https://github.com/marclijour/presentations

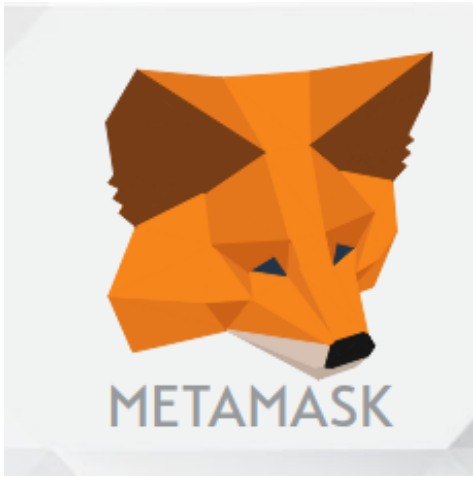
Table of Contents

Let's try things out!

Install MetaMask

Follow step by step:

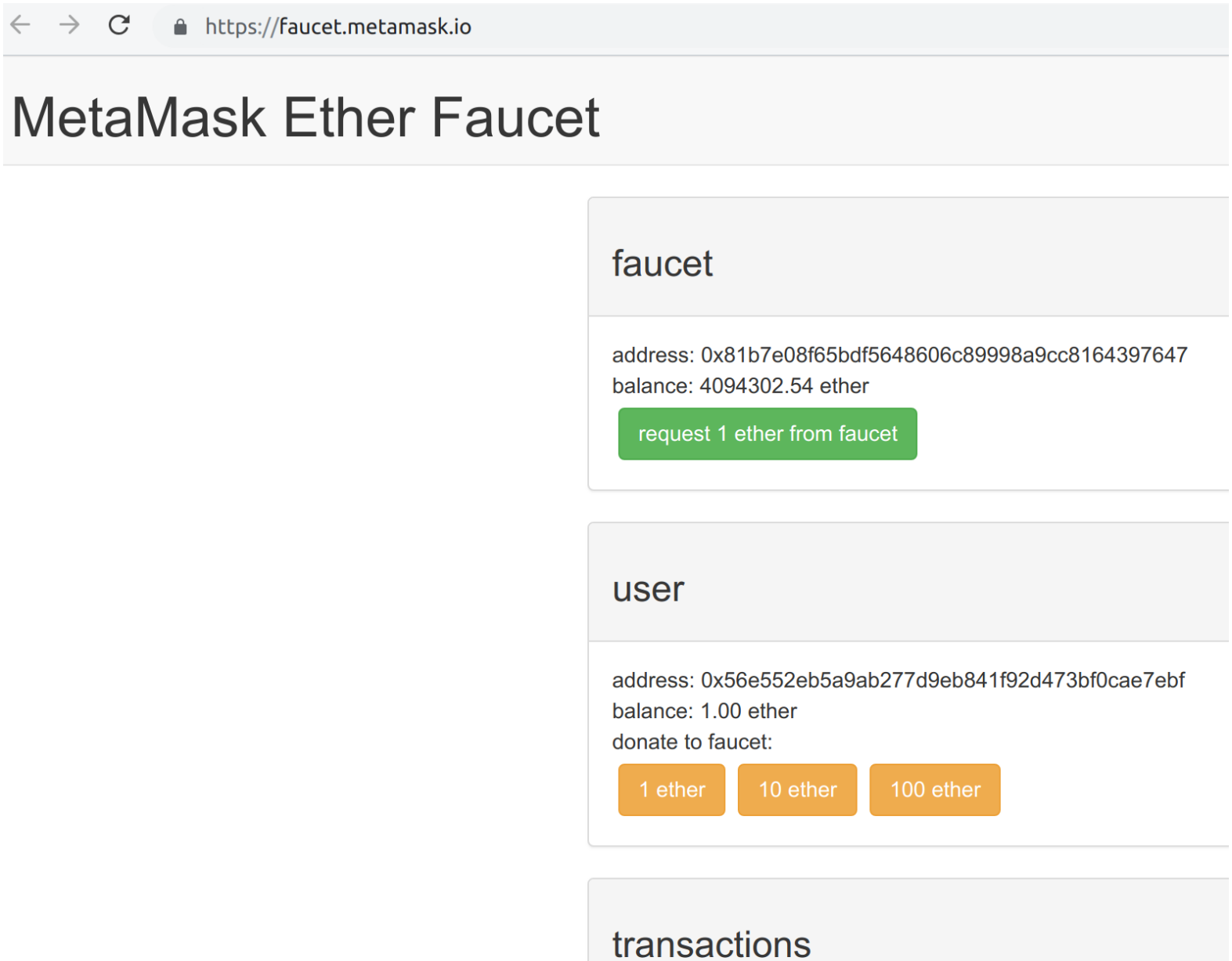
1. Install the Chrome/Chromium extension
2. Watch the intro on Youtube
3. Create an account
4. Switch to the Ropsten Testnet (top-right in MetaMask)
5. Fill your account with Ether from https://faucet.metamask.io



https://metamask.io

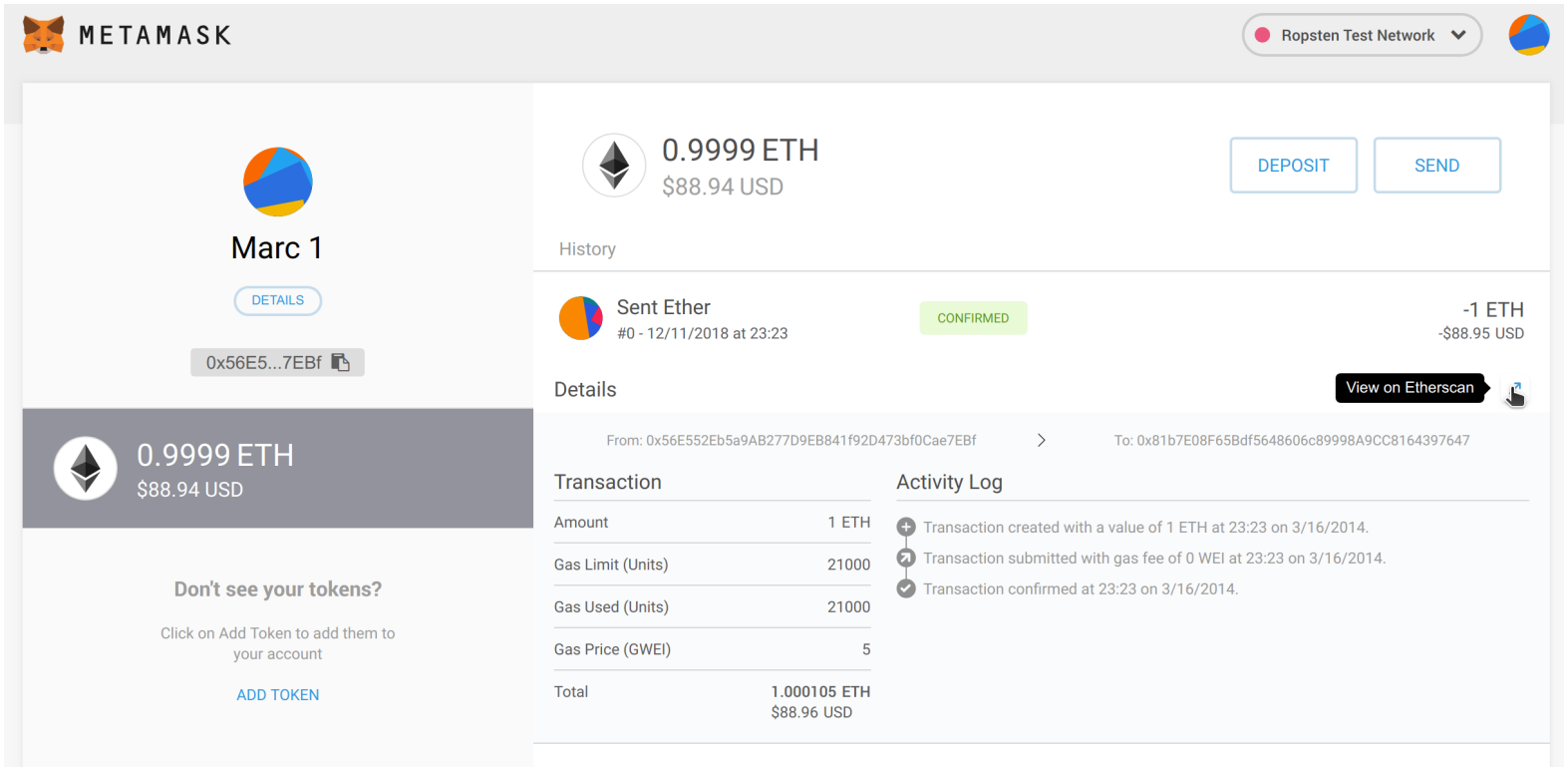
Request Ether from the faucet (on the Ropsten network)

Do it several times; then donate 1 ether to the faucet



Check the transaction on Metamask

Click on the transaction for a detailed view



Check the transaction on Etherscan

ROPSTEN Etherscan
The Ethereum Block Explorer

ROPSTEN (Revival) TESTNET | Search by Address / Txhash / Block / Token / Ens | GO | Language

HOME | BLOCKCHAIN | TOKEN | MISC

Transaction 0xa8a8f32539cb69bd3e506b6527fcc7d44c43cccead09b30b10a9891c99355a3d

Home / Transactions / Tx Info

Overview

Transaction Information

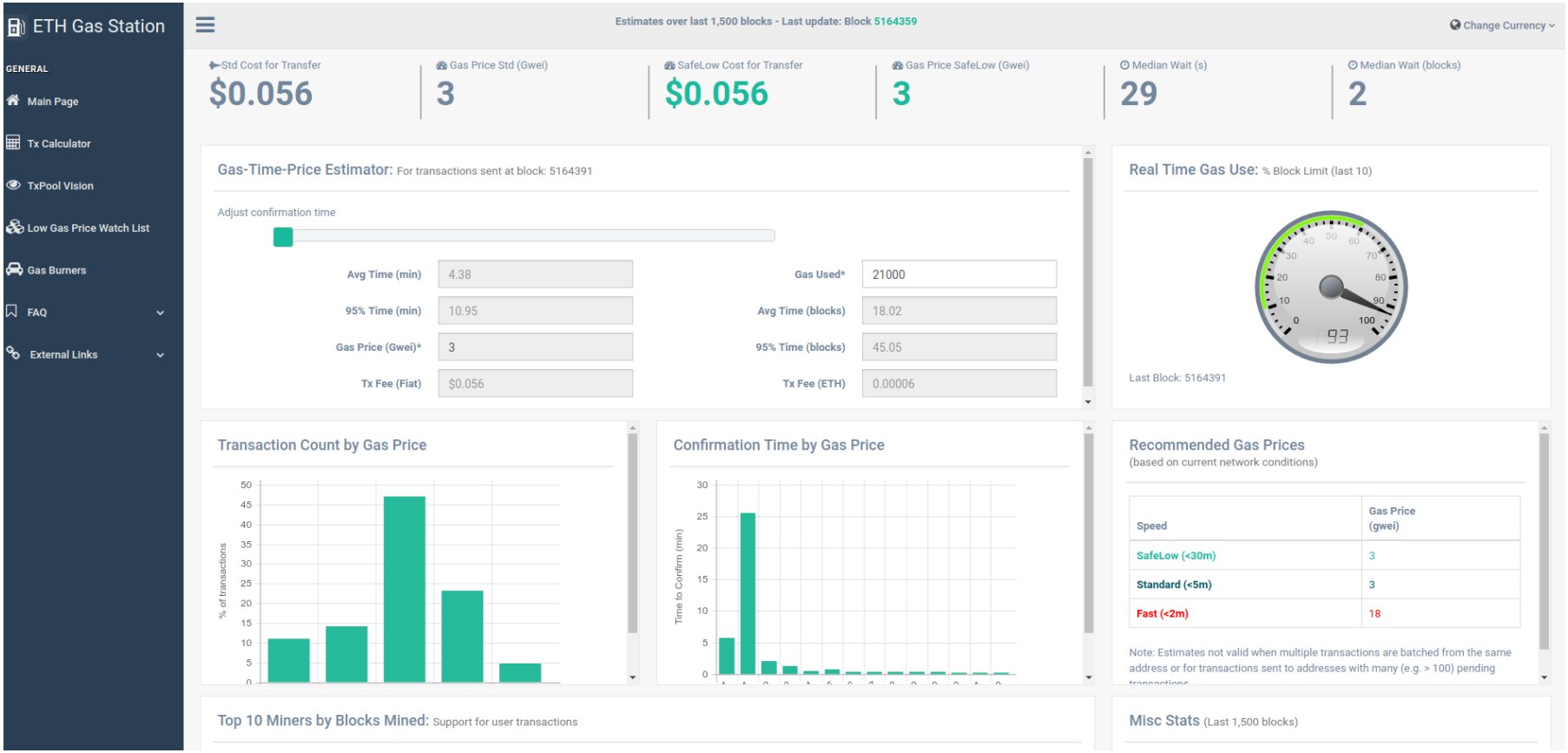
Tools & Utilities

[This is a Ropsten **Testnet** Transaction Only]

TxHash:	0xa8a8f32539cb69bd3e506b6527fcc7d44c43cccead09b30b10a9891c99355a3d
TxReceipt Status:	Success
Block Height:	4610407 (348 Block Confirmations)
TimeStamp:	1 hr 12 mins ago (Dec-12-2018 04:23:14 AM +UTC)
From:	0x56e552eb5a9ab277d9eb841f92d473bf0cae7ebf
To:	0x81b7e08f65bdf5648606c89998a9cc8164397647
Value:	1 Ether ($0.00)
Gas Limit:	21000
Gas Used By Transaction:	21000 (100%)
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	0.000105 Ether ($0.000000)
Nonce & {Position}:	0 | {6}
Input Data:	0x

A note about gas price

https://ethgasstation.info



Price of (real) ether: ETH

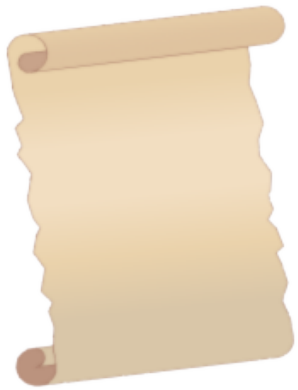
More information: https://www.tradingview.com/symbols/ETHUSD/

Wallets

More information: https://blockgeeks.com/guides/cryptocurrency-wallet-guide/

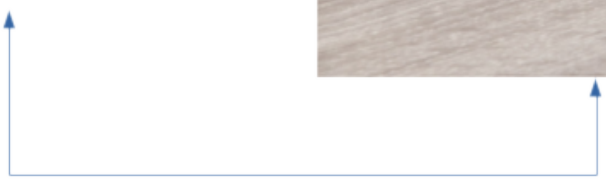
Software	Hardware	Paper

Jaxx



mycelium
ad-hoc economy

MyEtherWallet



Exchanges

1. Centralized Exchanges (Coinbase, Quadriga, ...)
2. Decentralized Exchanges

ATMs

More information: https://coinatmradar.com/country/138/bitcoin-atm-mexico/

Other crypto-assets

More information:

https://www.tradingview.com/markets/cryptocurrencies/prices-all/

Overview | Performance | Oscillators | Trend-Following | USD BTC

NAME 301 matches	MKT CAP	FD MKT CAP	LAST	AVAIL COINS	TOTAL COINS	TRADED VOL	CHG %
Bitcoin	59.852B	72.158B	3436.1	17.419M	21M	4.712B	0.02%
XRP	12.167B	29.729B	0.29729	40.927B	100B	369.224M	0.17%
Ethereum	9.257B	9.257B	89.23	103.745M	103.745M	1.739B	0.10%
Stellar	2.165B	11.811B	0.11297826	19.165B	104.543B	197.41M	-0.34%
Tether	1.838B	2.554B	0.99000000	1.856B	2.58B	2.97B	-0.10%
Bitcoin Cash	1.729B	2.074B	98.760	17.506M	21M	71.709M	0.92%
EOS	1.692B	1.879B	1.8672	906.245M	1.006B	740.947M	0.44%
Bitcoin SV	1.548B	1.858B	88.45300000	17.505M	21M	59.813M	-2.60%
Litecoin	1.431B	2.02B	24.045	59.532M	84M	380.518M	1.14%
TRON	877.572M	1.314B	0.013247	66.247B	99.218B	72.465M	-0.88%
Cardano	772.388M	1.341B	0.029791	25.927B	45B	9.766M	-0.09%
Monero	722.858M	722.858M	43.445	16.638M	16.638M	11.502M	1.38%
NEM	642.663M	642.663M	0.07141	9B	9B	8.23M	-1.53%
Binance Coin	635.009M	926.299M	4.8548350	130.799M	190.799M	20.772M	-2.52%
IOTA	631.509M	631.509M	0.2272	2.78B	2.78B	4.203M	1.07%
Dash	554.925M	1.234B	65.28257000	8.5M	18.9M	160.684M	2.12%
Ethereum Classic	402.997M	402.997M	3.777	106.698M	106.698M	106.521M	0.68%
NEO	387.602M	596.31M	5.96	65M	100M	100.484M	1.51%

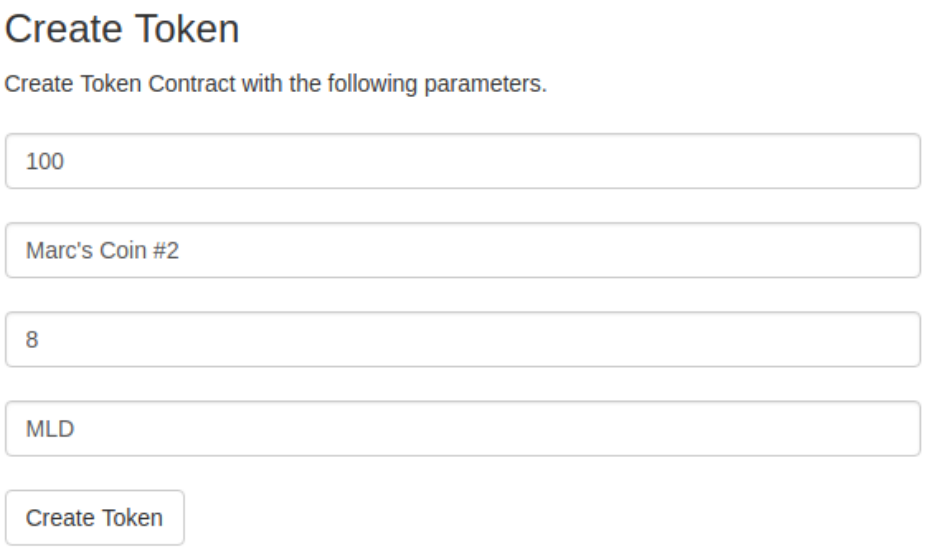
Ethereum, Alt-Coins, and ICOs

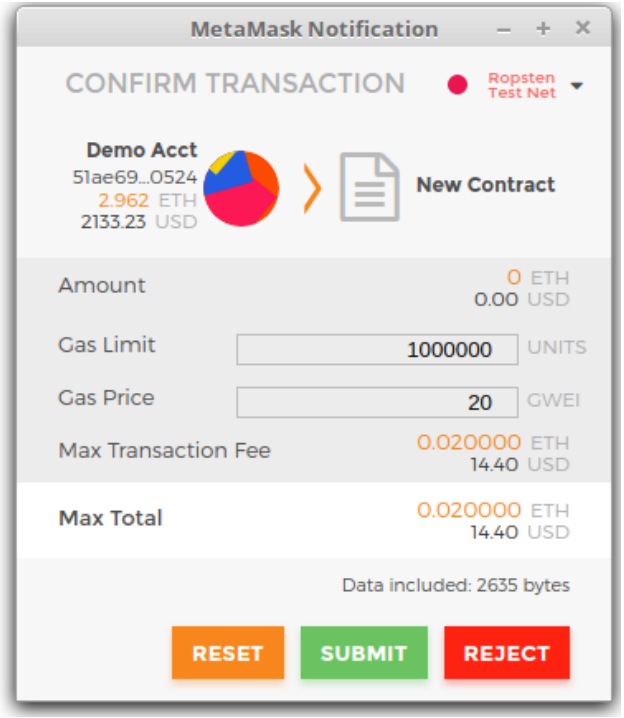
1. 94% of the top 100 tokens are built on top of Ethereum
2. $5.5 billion raised in 2017
3. $6.5 billion raised in the first quarter of 2018
4. Ethereum has the largest developer community
5. Close to 2,000 dapps (decentralized applications) counted on Ethereum

Crypto as seen by the Regulator (and the taxman)

1. Cryptocurrency
2. Utility Token
3. Security Token

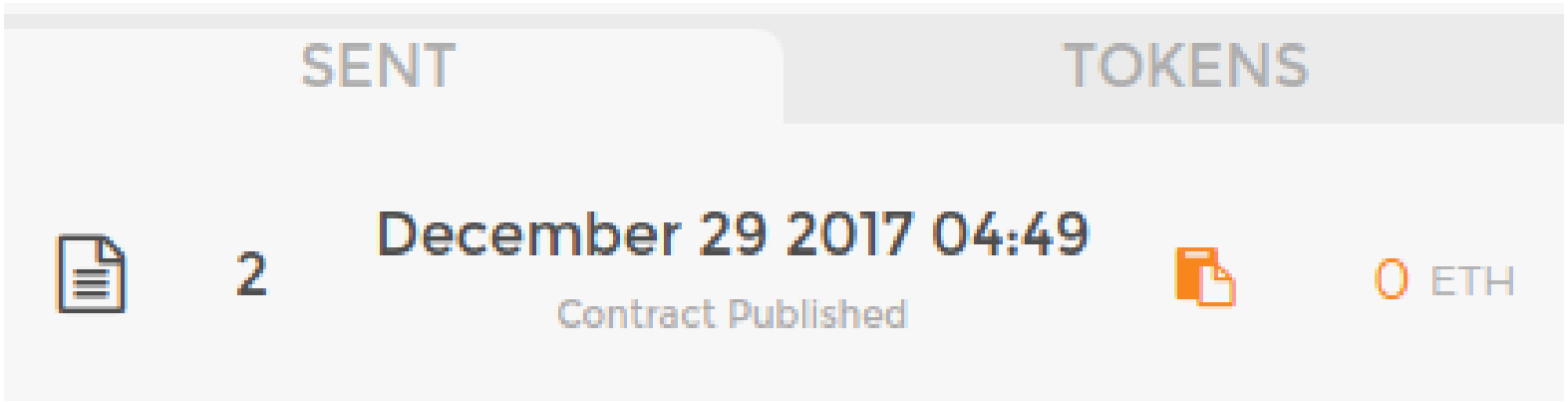
Create your own (ERC-20) token





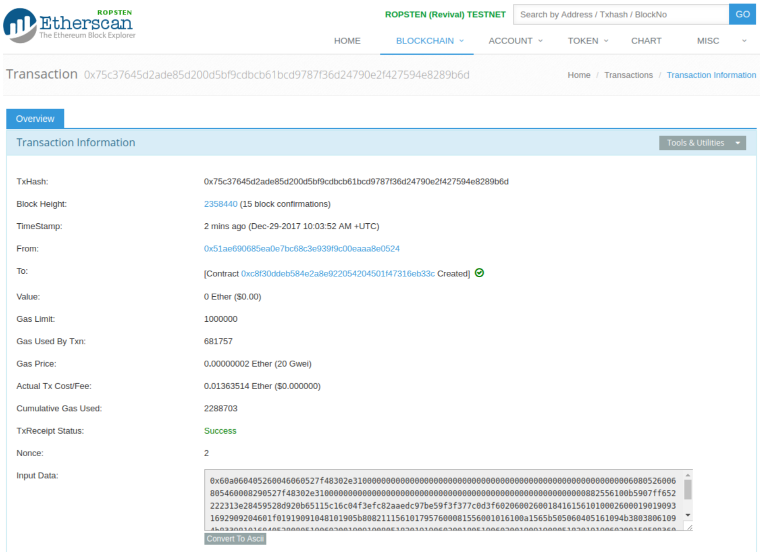
1. Use the Token Factory Dapp at https://tokenfactory.surge.sh/#/factory
2. MetaMask will pop up (see picture above)
3. Submit the transaction (on the Ropsten Testnet)
4. Check your transaction on https://ropsten.etherscan.io

Check your Smart Contract



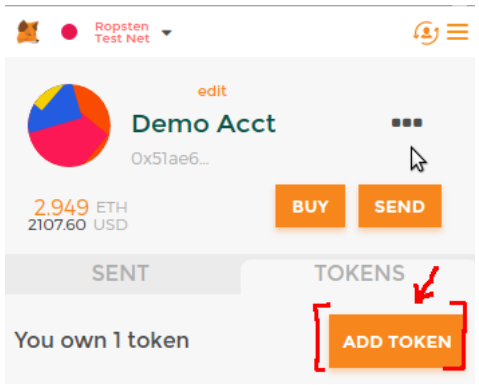
1. Select the "Sent" tab
2. Check the orange Copy icon (Tx Hash)
3. Click on "Contract Published"
4. That should bring you to Etherscan (see next page)

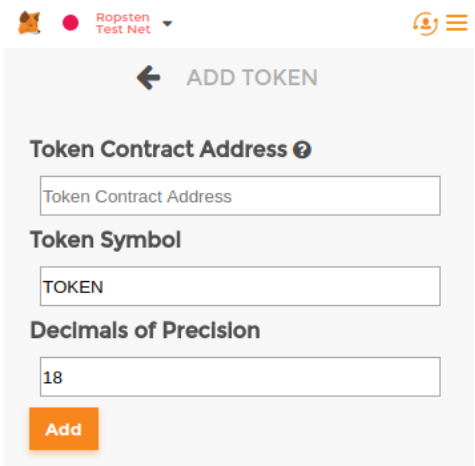
Verify the status of your transaction on Etherscan



Transaction Information: note the "To" line with your contract address

Watch your Token





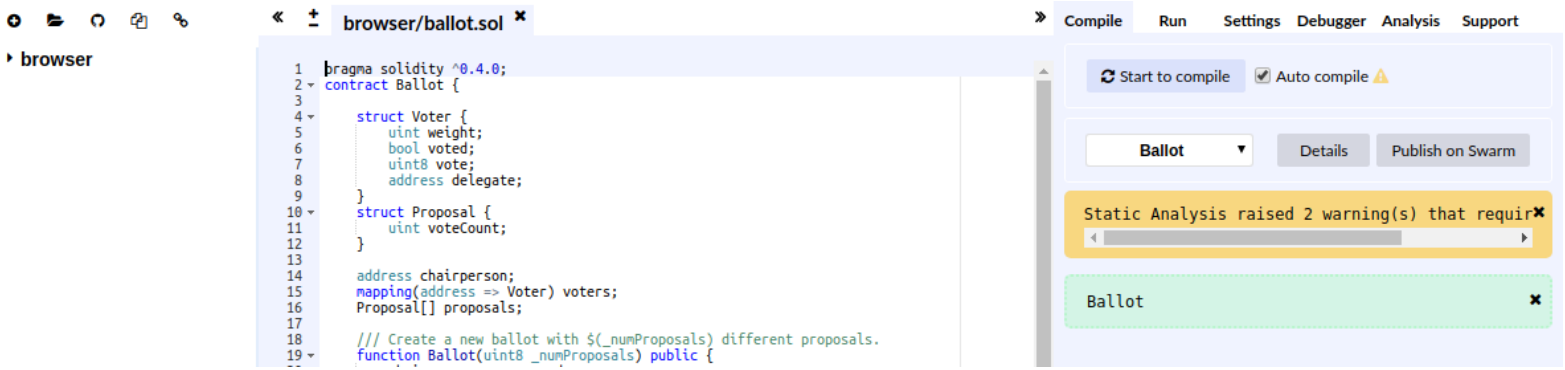
1. Click on the "Add Token" button
2. Wait for the next window (picture on the right)
3. Copy your contract address (from Etherscan)
4. Go back to your Token Factory tab, which should show an UI to interact with your contract or go to the URL: https://tokenfactory.surge.sh/#/token/0x... (replace 0x... by your contract address)
5. Move coins around
6. In MetaMask, click on your token to check the tx on Etherscan

Table of Contents

Remember: Ethereum

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.
— https://ethereum.org

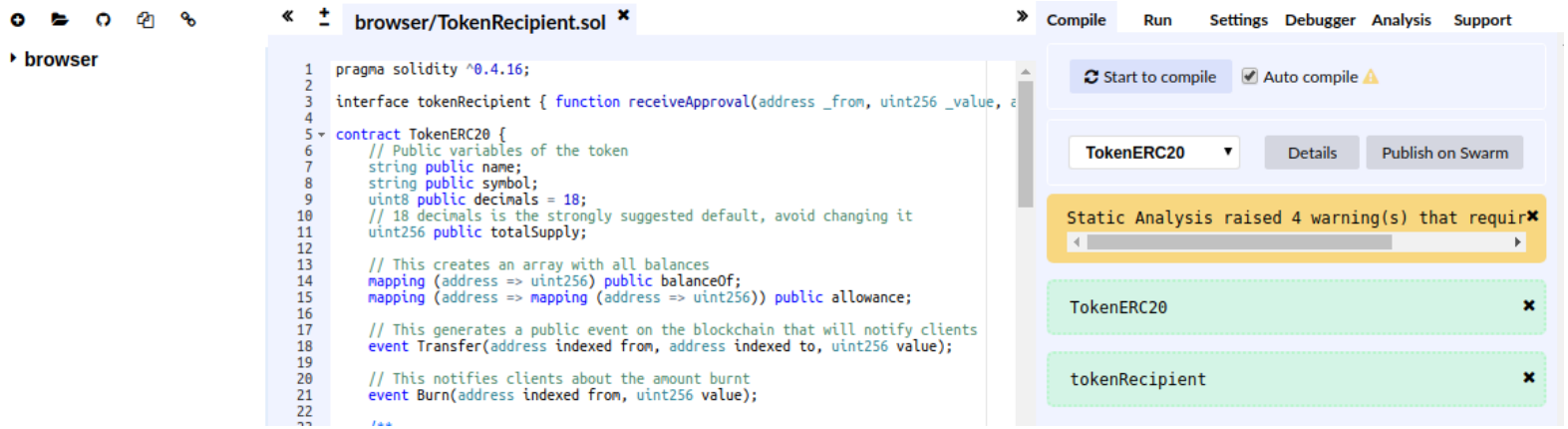
Coding your first ERC-20 Smart Contract



1. Open the Remix IDE at https://remix.ethereum.org
2. Close the ballot file
3. Create a new file named TokenRecipient.sol
4. Copy the code from https://ethereum.org/token (second white box, under "The Code", starting with "pragma")
5. Switch to the "Run" tab (top-right bar, after Compile)

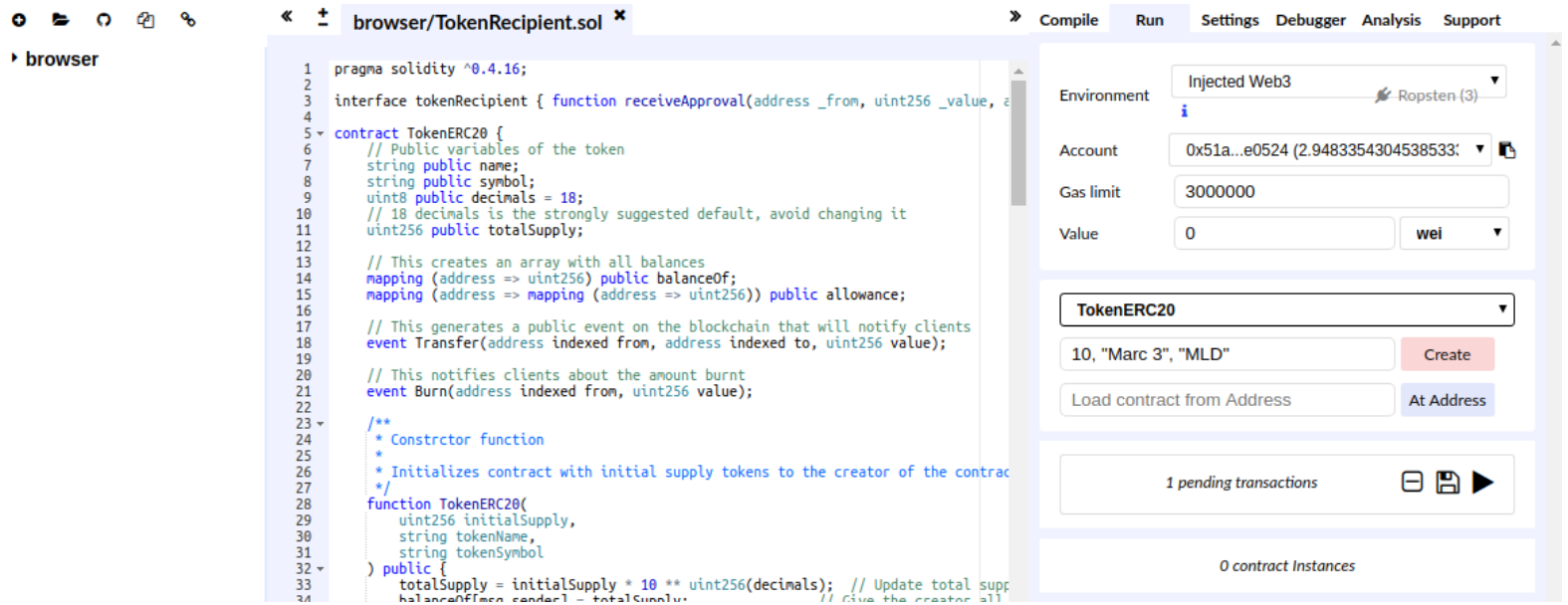
Reference:
ERC-20 Token Standard

Compiling Successfully



1. Two green boxes should show on the right
2. TokenERC20 is the name of the contract (class)
3. tokenRecipient is the name of the interface
4. Switch to the "Run" tab (top right)

Submitting the Smart Contract

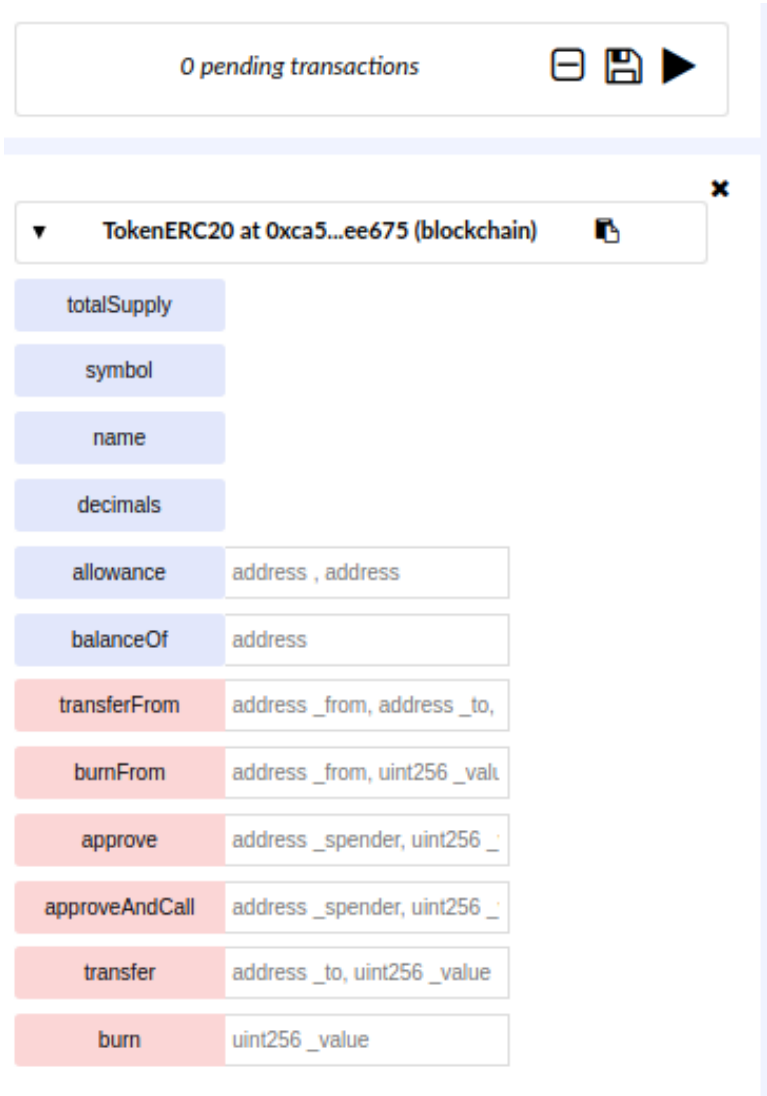



```
pragma solidity ^0.4.16;

interface tokenRecipient { function receiveApproval(address _from, uint256 _value, a

contract TokenERC20 {
    // Public variables of the token
    string public name;
    string public symbol;
    uint8 public decimals = 18;
    // 18 decimals is the strongly suggested default, avoid changing it
    uint256 public totalSupply;

    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;
    mapping (address => mapping (address => uint256)) public allowance;

    // This generates a public event on the blockchain that will notify clients
    event Transfer(address indexed from, address indexed to, uint256 value);

    // This notifies clients about the amount burnt
    event Burn(address indexed from, uint256 value);

    /**
     * Constrctor function
     *
     * Initializes contract with initial supply tokens to the creator of the contrac
     */
    function TokenERC20(
        uint256 initialSupply,
        string tokenName,
        string tokenSymbol
    ) public {
        totalSupply = initialSupply * 10 ** uint256(decimals);  // Update total supp
```

1. Under the dropdown showing "TokenERC20", add a number (total amount of tokens to issue) and two strings (the latter is the token symbol)
2. Add enough gas (top right, try 30)
3. Click Create and check whether MetaMask needs confirmation

Interacting with the contract

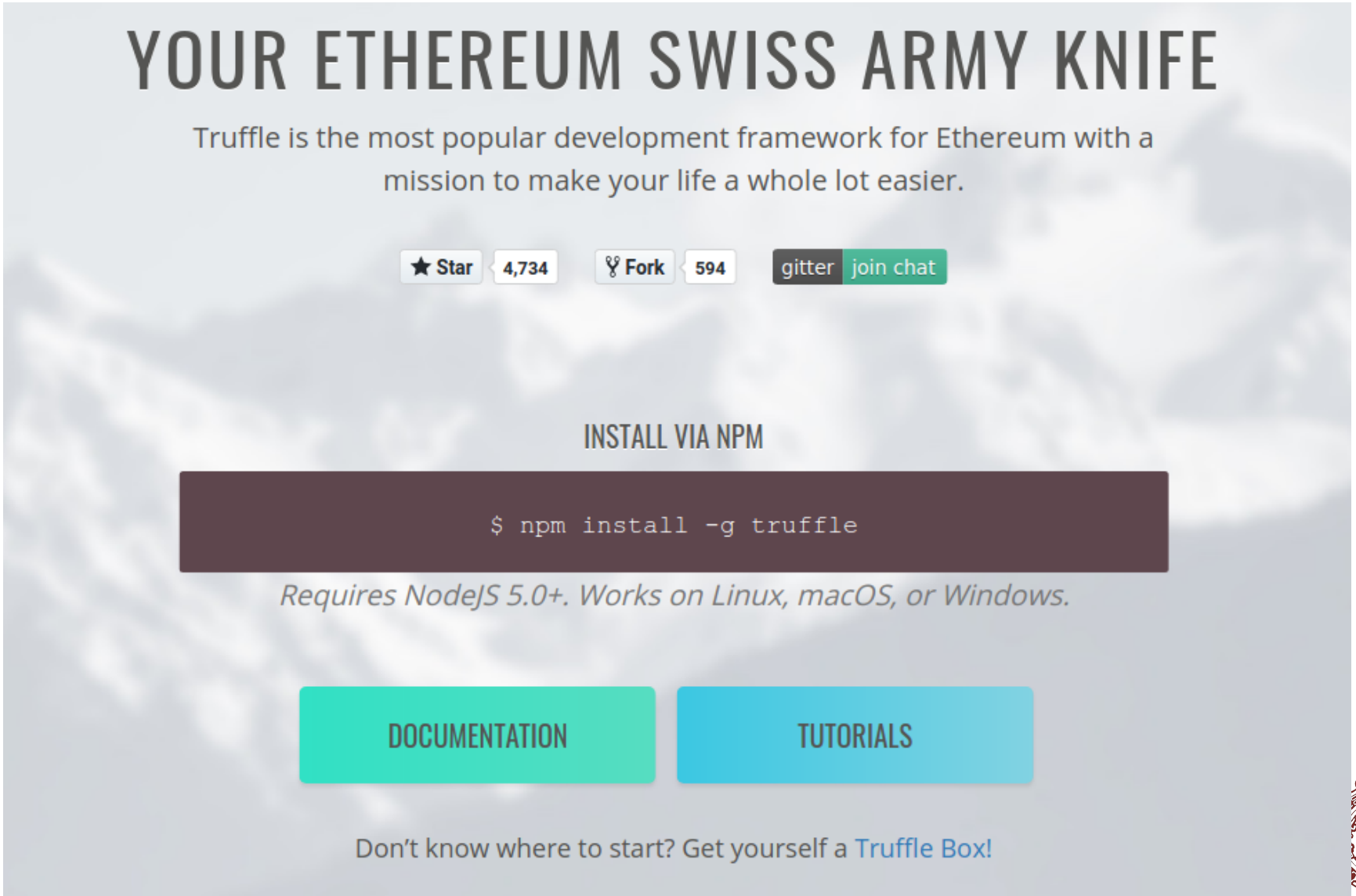
1. A new interface will pop up on the bottom right corner of the IDE



Tools for Developers

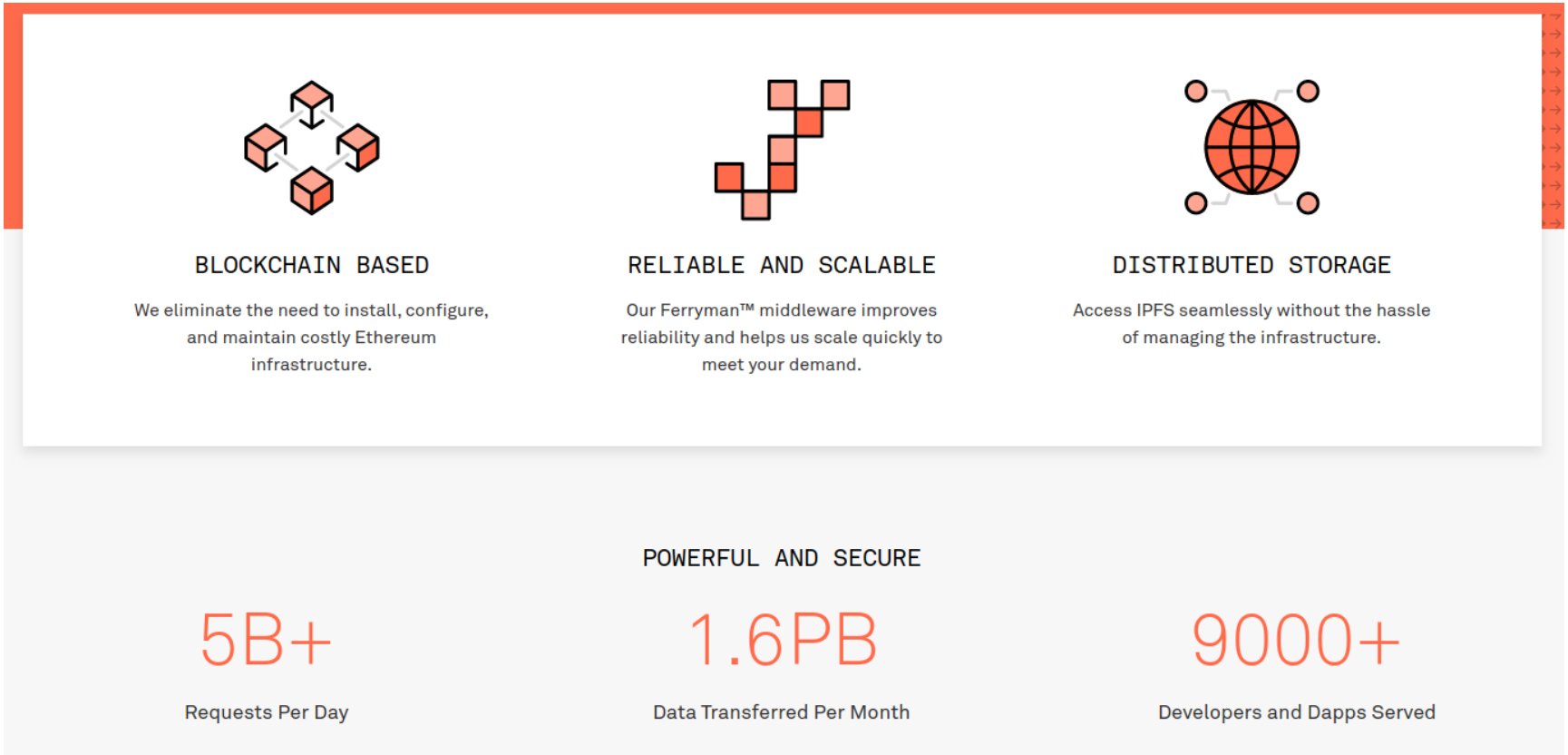
Truffle Framework

http://truffleframework.com



Infura

http://infura.io



Mythril

https://github.com/ConsenSys/mythril

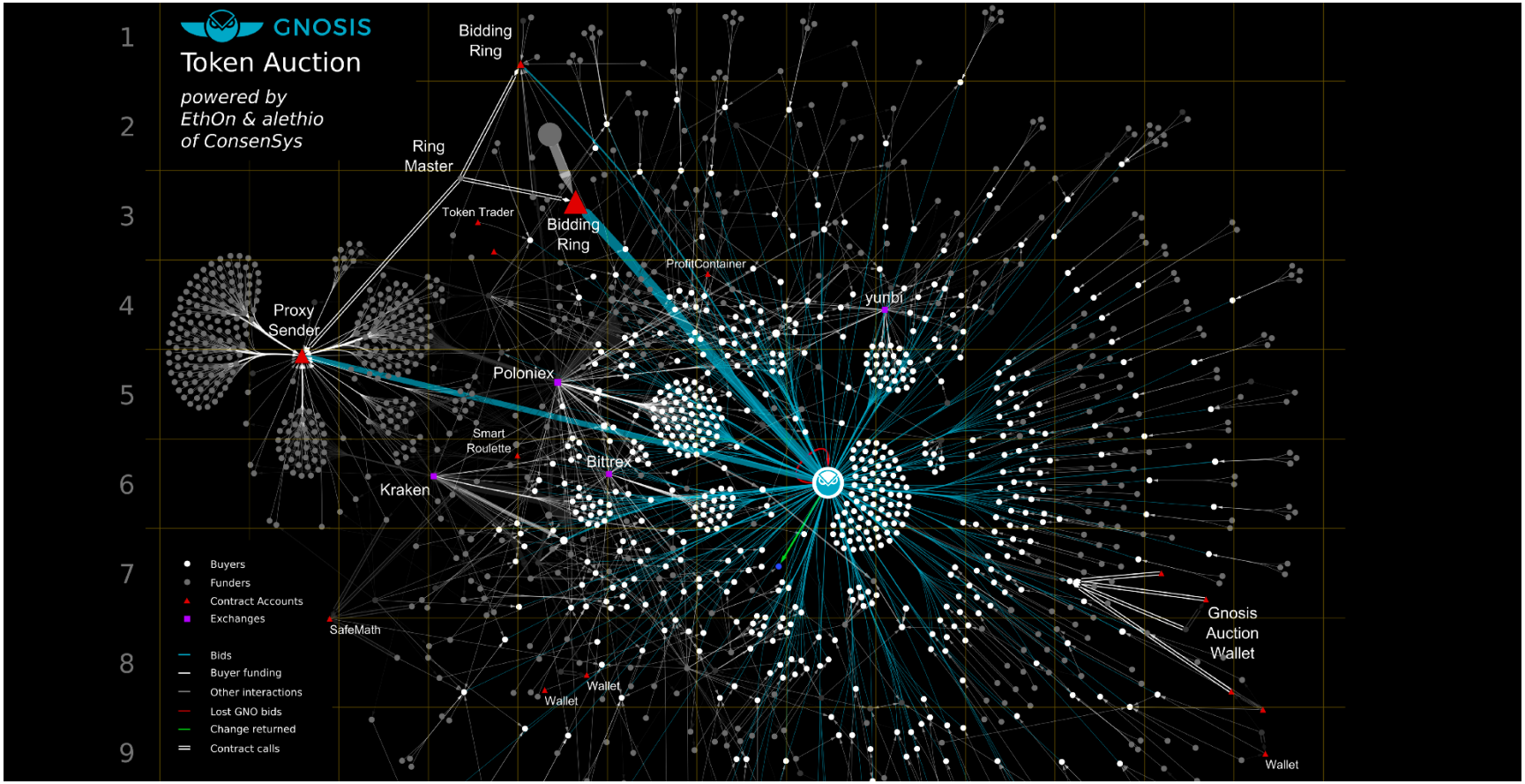
Mythril is a security analysis tool for smart contracts.
It comes as a Python package that requires a solidity compiler and a C++ compiler.

```
$ sudo apt install libssl-dev
$ sudo apt install gcc g++
$ sudo add-apt-repository ppa:ethereum/ethereum
$ sudo apt install solc
$ sudo pip3 install mythril
$ myth -x contracts/higherbidder.sol
```

See also https://hackernoon.com/introducing-mythril-a-framework-for-bug-hunting-on-the-ethereum-blockchain-9dc5588

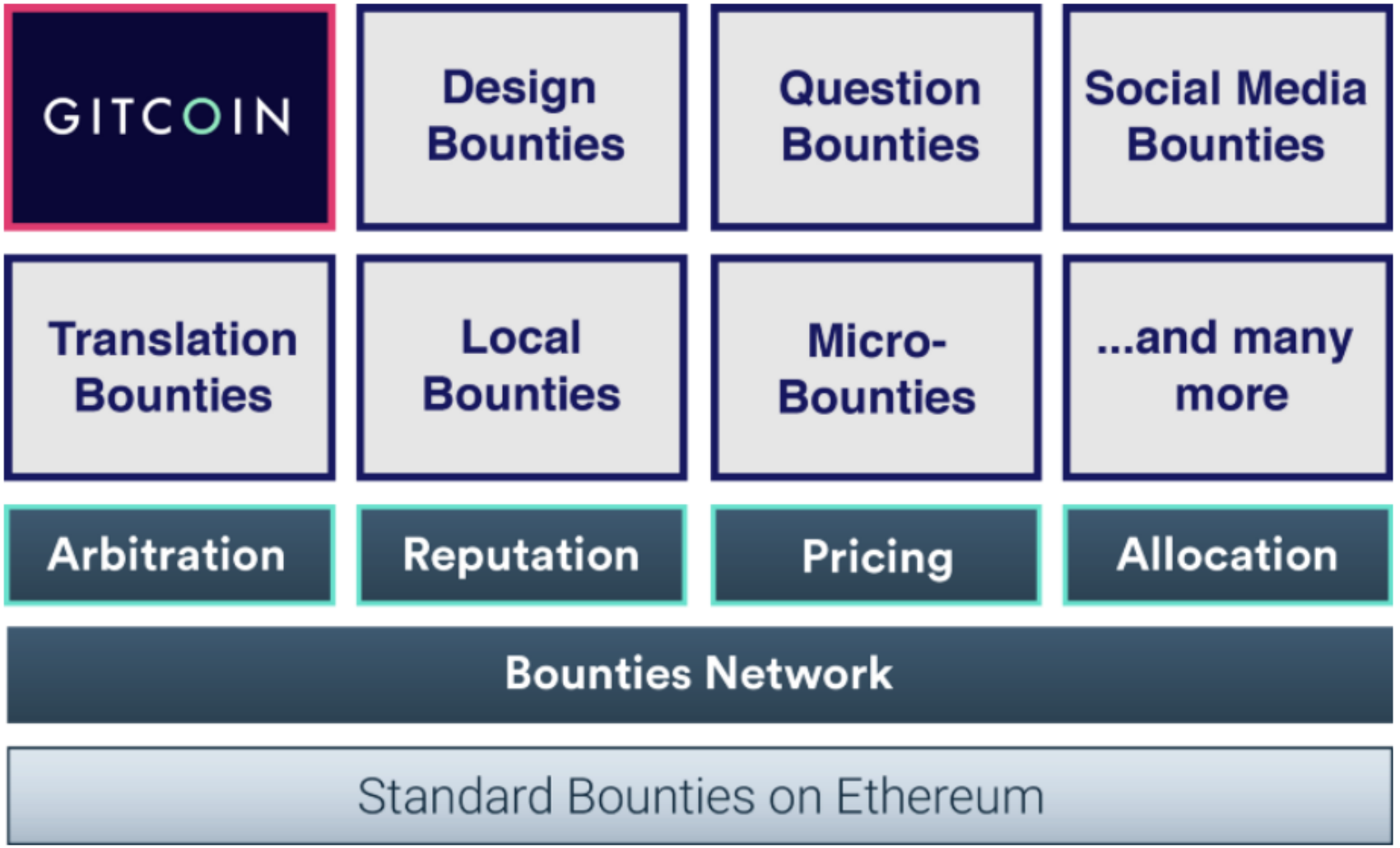
Big Data and Analytics on Ethereum

https://aleth.io



Getting paid for your work: The Bounties Network

https://bounties.network



Gitcoin (depth-first) and Bounties Network (breadth-first) have integrated!

Gitcoin

https://gitcoin.co

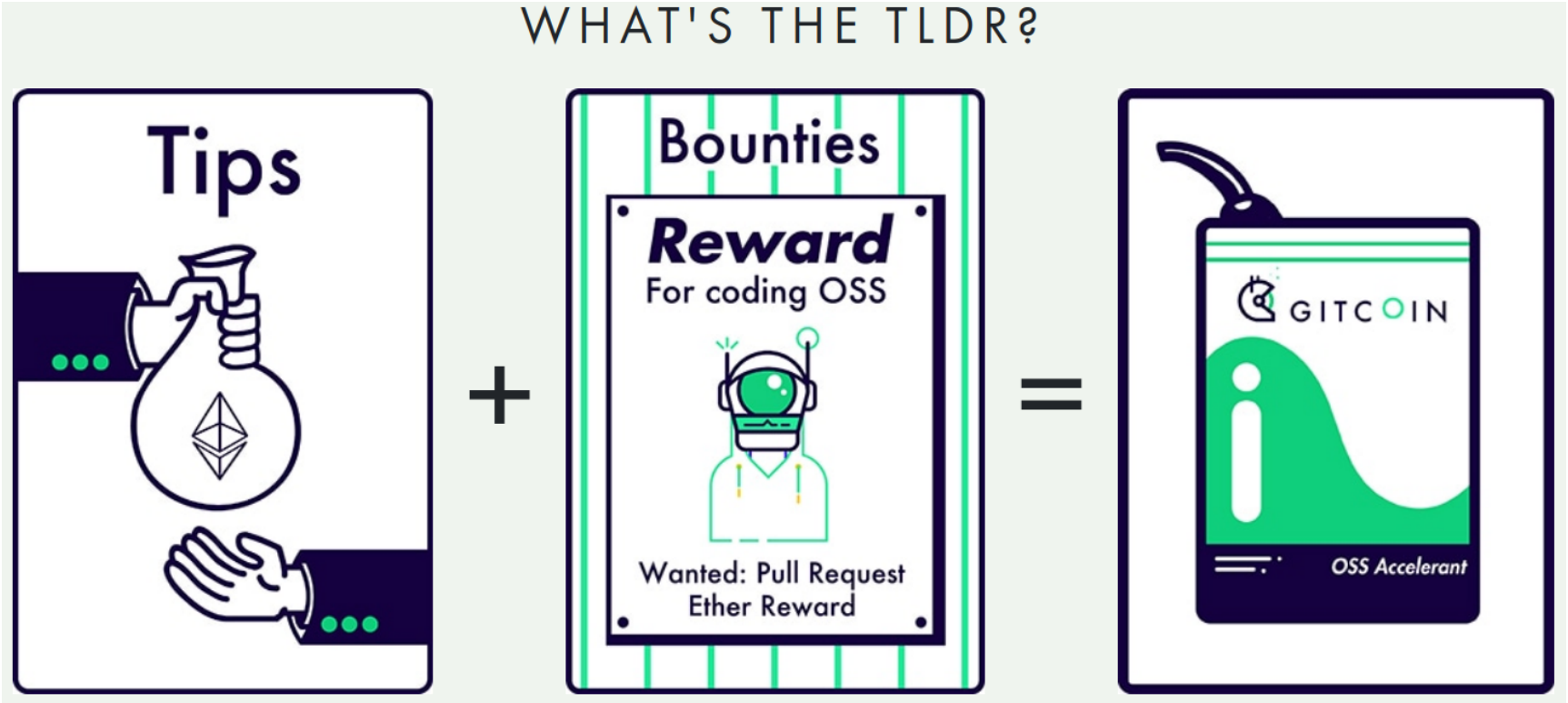
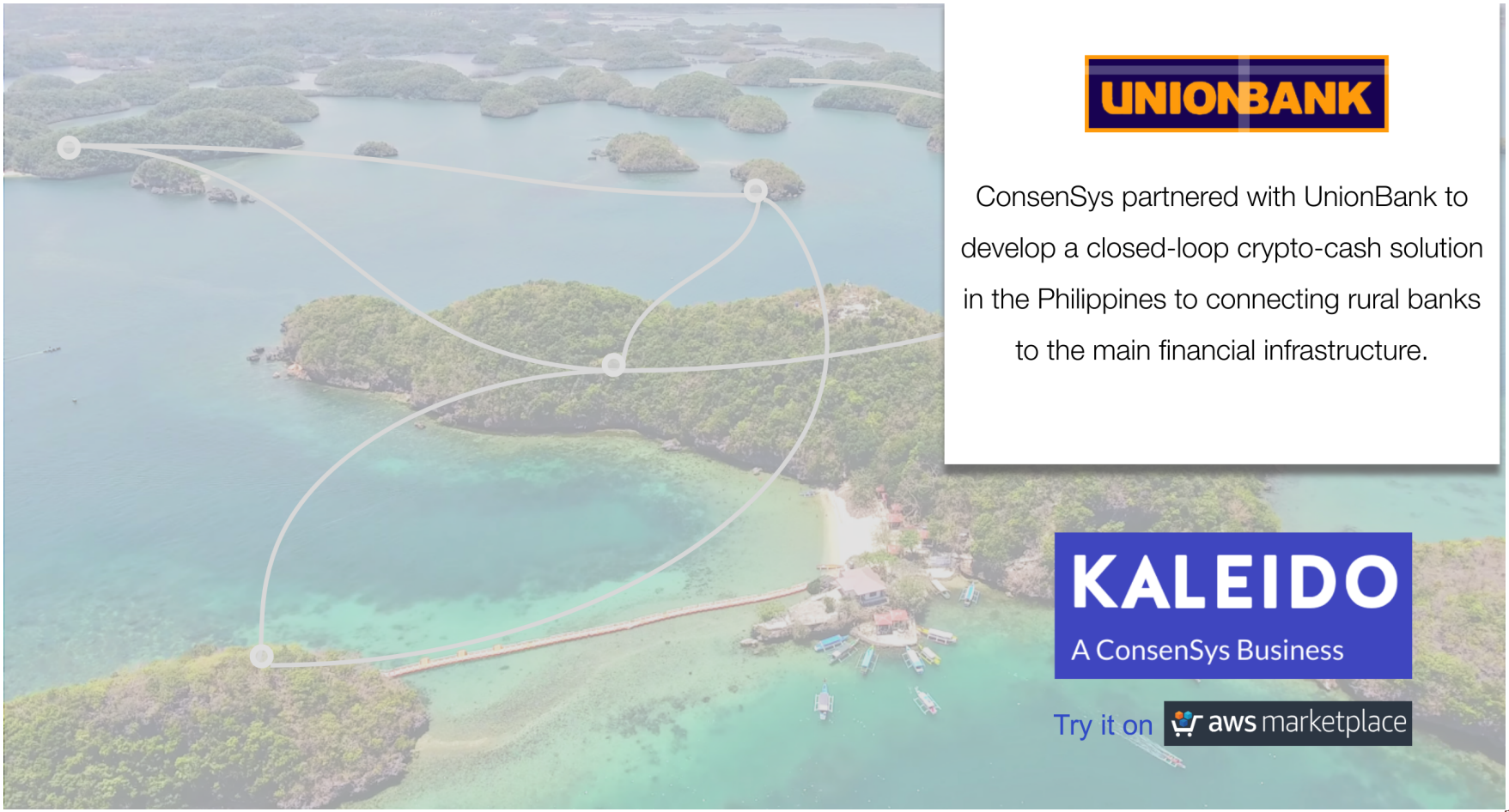


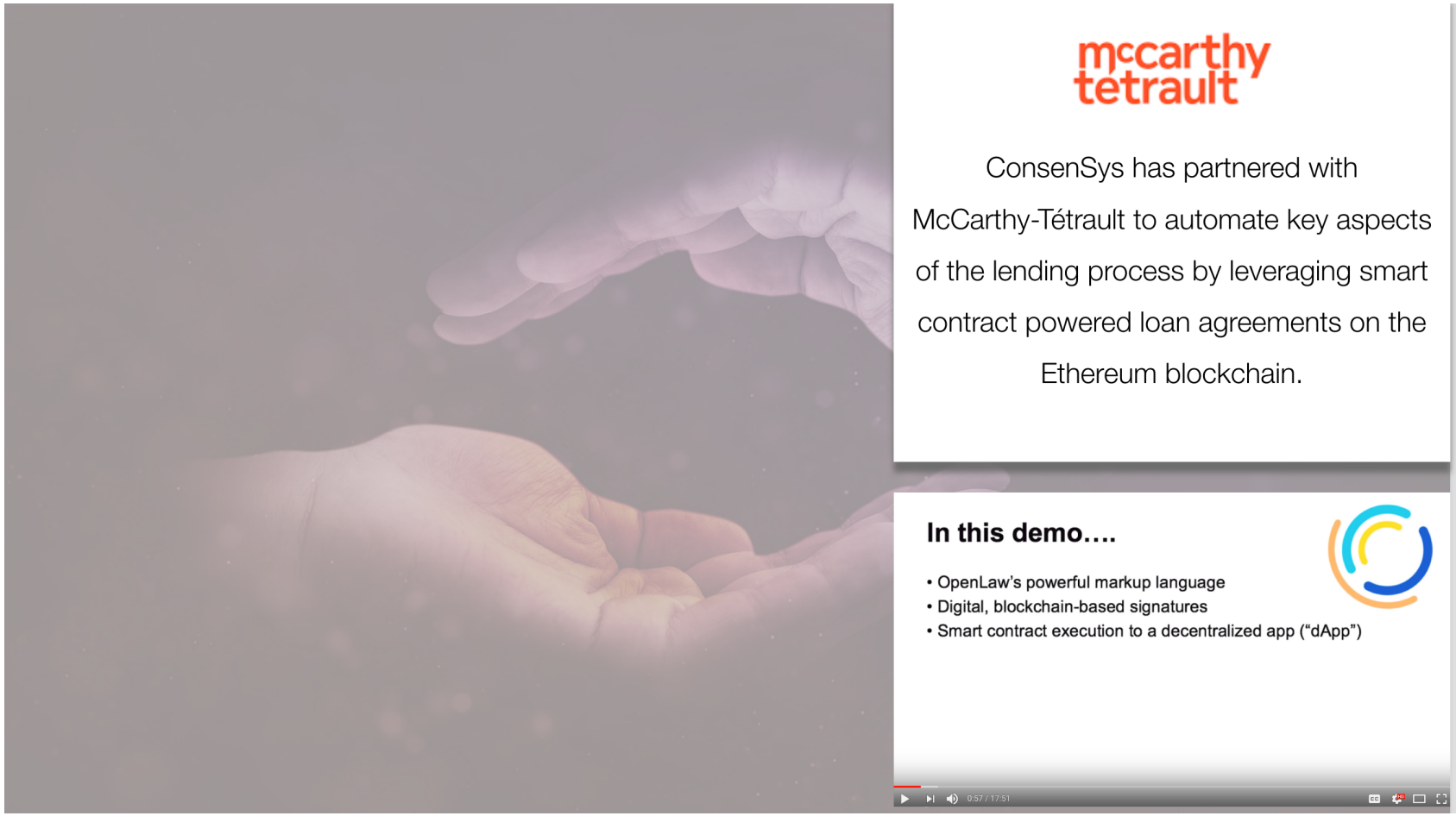
Table of Contents

Transforming Industries

Transforming Industries



Transforming Industries



Thank you!

Email: marc@lijour.net

Twitter: @marclijour

References