



Ayana
Consulting

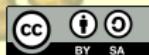
An Introduction to Blockchain and Ethereum

A primer

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/2yh9xuG>

or find by date:

<https://github.com/marclijour/presentations>



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>



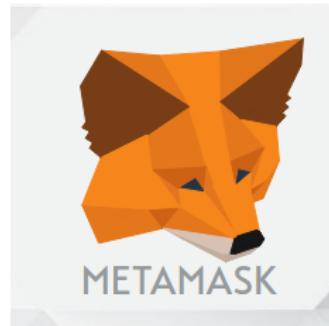
Let's try things out!



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-left 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)

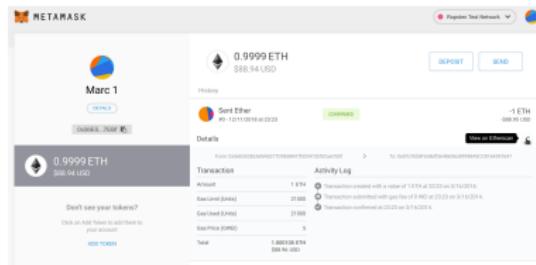
Do it several times to get more than 1 ether in your account; then donate 1 ether to the faucet

..../pics/ethereum/faucet-ropsten.png



Check the transaction on Metamask

Click on the transaction for a detailed view



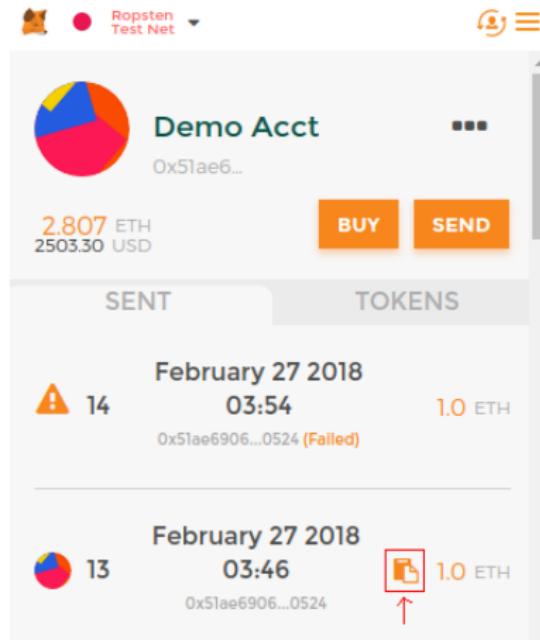
Try sending ETH to yourself with Metamask

- ① Make sure you're on Ropsten, with some ETH from the faucet
- ② Click on "Send" and fill:
 - Account: paste your own address (same account)
 - Amount: 1 ETH
 - Transaction data: convert some text in HEX format with
<https://www.asciitohex.com>, remove all spaces and write it with a 0x prefix (e.g. 0x497427732074696d6520746f2072756e)
- ③ Click on "Next"
- ④ Use a gas price > 30 (the higher the faster)
- ⑤ Confirm the transaction



Check the transaction on Etherscan

Copy the transaction #



Check the transaction on Etherscan

and click on "Convert to Ascii"



ROPSTEN

0x023983a0a803e906879dab806d4ada22a7776445264c8f671f92ead92415d65b

GO

HOME

BLOCKCHAIN ▾

ACCOUNT ▾

TOKEN ▾

CHART

MISC ▾

Transaction 0x023983a0a803e906879dab806d4ada22a7776445264c8f671f92ead92415d65b

Home / Transactions / Transaction Information

Overview

Transaction Information

Tools & Utilities ▾

TxHash: 0x023983a0a803e906879dab806d4ada22a7776445264c8f671f92ead92415d65b

TxReceipt Status: Success

Block Height: 2735788 (76 block confirmations)

TimeStamp: 23 mins ago (Feb-27-2018 08:47:28 AM +UTC)

From: 0x51ae690685ea0e7bc68c3e939f9c00eaaa8e0524

To: 0x51ae690685ea0e7bc68c3e939f9c00eaaa8e0524

Value: 1 Ether (\$0.00)

Gas Limit: 51000

Gas Used By Txn: 22088

Gas Price: 0.00000004 Ether (40 Gwei)

Actual Tx Cost/Fee: 0.00088352 Ether (\$0.000000)

Cumulative Gas Used: 58002

Nonce: 13

Input Data: 0x497427732074696d6520746f2072756e

Convert To Ascii



A note about gas price

<https://ethgasstation.info>

ETH Gas Station

Estimates over last 1,500 blocks - Last update: Block 5164391

Change Currency ▾

Std Cost for Transfer \$0.056 | **Gas Price Std (wei)** 3 | **SafeLow Cost for Transfer** \$0.056 | **Gas Price SafeLow (wei)** 3 | **Median Wait (s)** 29 | **Median Wait (blocks)** 2

Gas-Time-Price Estimator: For transactions sent at block: 5164391

Adjust confirmation time

Avg Time (m/s)	4.38
95% Time (m/s)	10.95
Gas Price (Wei)*	3
Tx Fee (Flat)	\$0.056

Gas Used*	21000
Avg Time (blocks)	18.02
95% Time (blocks)	45.05
Tx Fee (ETH)	0.00005

Real Time Gas Use: % Block Limit (last 10)

Last Block: 5164391

Transaction Count by Gas Price

Confirmation Time by Gas Price

Recommended Gas Prices (based on current network conditions)

Speed	Gas Price (wei)
SafeLow (<30m)	3
Standard (<5m)	3
Fast (<2m)	18

Note: Estimates not valid when multiple transactions are batched from the same address or for transactions sent to addresses with many (e.g. > 100) pending nonce conflicts.

Misc Stats (Last 1,500 blocks)

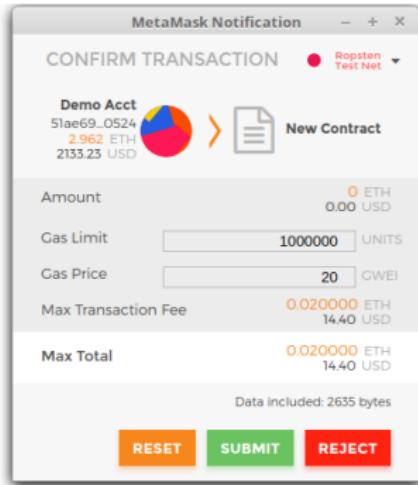


Create your own (ERC-20) token

Create Token

Create Token Contract with the following parameters.

100
Marc's Coin #2
8
MLD
<input type="button" value="Create 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

A screenshot of a blockchain transaction history interface. At the top, there are two tabs: "SENT" (selected) and "TOKENS". Below the tabs, the date "December 29 2017 04:49" is displayed. To the left of the date is a document icon with the number "2" next to it, indicating two contracts have been published. To the right of the date is an orange copy icon with "0 ETH" next to it, indicating no ether was sent. The text "Contract Published" is centered below the date.

- 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)

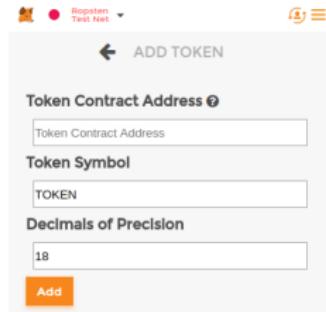
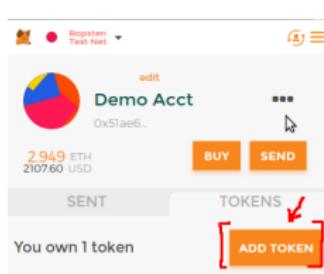


Verify the status of your transaction on Etherscan

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



Too easy?

Let's code it in Solidity
like the pros!



Coding your first ERC-20 Smart Contract

The screenshot shows the Remix IDE interface. On the left, there's a file tree with a single item: 'browser/ballot.sol'. The main area displays the Solidity code for the 'Ballot' contract. The code defines a struct 'Voter' with fields 'uint weight', 'bool voted', 'uint8 vote', and 'address delegate'. It also defines a struct 'Proposal' with fields 'uint voteCount' and 'address chairperson'. A mapping 'mapping(address => Voter) voters;' is declared, along with a dynamic array 'Proposal[] proposals;'. A constructor function 'Ballot(uint8 _numProposals)' is defined with a note: '/// Create a new ballot with \${_numProposals} different proposals.' At the bottom of the code editor, there are several tabs: 'Compile', 'Run', 'Settings', 'Debugger', 'Analysis', and 'Support'. The 'Run' tab is currently selected. In the top right corner, there are buttons for 'Start to compile' (with 'Auto compile' checked), 'Compile', 'Run', 'Settings', 'Debugger', 'Analysis', and 'Support'. Below these buttons, there are tabs for 'Ballot' (selected), 'Details', and 'Publish on Swarm'. A yellow warning box at the bottom states 'Static Analysis raised 2 warning(s) that require fixing'. A green box below it says 'Ballot'.

```
pragma solidity ^0.4.0;
contract Ballot {
    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
        address chairperson;
    }
    mapping(address => Voter) voters;
    Proposal[] proposals;
    // Create a new ballot with ${_numProposals} different proposals.
    function Ballot(uint8 _numProposals) public {
```

- 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

The screenshot shows the Truffle UI interface. On the left, there's a code editor window titled "browser/TokenRecipient.sol" containing Solidity code. On the right, there's a toolbar with tabs for "Compile", "Run", "Settings", "Debugger", "Analysis", and "Support". Below the toolbar, a message says "Start to compile" with an "Auto compile" checkbox. Underneath, it shows "TokenERC20" selected in a dropdown, with "Details" and "Publish on Swarm" buttons. A yellow box indicates "Static Analysis raised 4 warning(s) that require attention". Below this, two green boxes are listed: "TokenERC20" and "tokenRecipient".

```
1 pragma solidity ^0.4.16;
2
3 interface tokenRecipient { function receiveApproval(address _from, uint256 _value, i
4
5+ contract TokenERC20 {
6+     // Public variables of the token
7+     string public name;
8+     string public symbol;
9+     uint8 public decimals = 18;
10+    // 18 decimals is the strongly suggested default, avoid changing it
11+    uint256 public totalSupply;
12+
13+    // This creates an array with all balances
14+    mapping (address => uint256) public balanceOf;
15+    mapping (address => mapping (address => uint256)) public allowance;
16+
17+    // This generates a public event on the blockchain that will notify clients
18+    event Transfer(address indexed from, address indexed to, uint256 value);
19+
20+    // This notifies clients about the amount burnt
21+    event Burn(address indexed from, uint256 value);
22+
23+}
```

- 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

The screenshot shows the Truffle UI interface. On the left, the code editor displays the Solidity code for `TokenERC20.sol`. The code defines a contract with variables for name, symbol, and totalSupply, and includes functions for receiving approvals, transferring tokens, and burning tokens. On the right, the deployment interface shows the environment set to "Injected Web3" with account 0x51a...e0524 selected. The gas limit is set to 3000000 and the value to 0 wei. A dropdown menu is open, showing "TokenERC20" selected. Below it, there's a "Create" button and a "Load contract from Address" field. At the bottom, it shows 1 pending transaction and 0 contract instances.

```
pragma solidity ^0.4.16;

interface TokenRecipient {
    function receiveApproval(address _from, uint256 _value, string _tokenName, string _tokenSymbol);
}

contract TokenERC20 {
    // Public variables of the token
    string public name;
    string public symbol;
    uint256 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);

    /**
     * Constructor function
     * Initializes contract with initial supply tokens to the creator of the contract
     */
    function TokenERC20(
        uint256 initialSupply,
        string tokenName,
        string tokenSymbol
    ) public {
        totalSupply = initialSupply * 10 ** uint256(decimals); // Update total supply
        balances[From] = initialSupply; // Give the creator all
    }
}
```

- 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

0 pending transactions

TokenERC20 at 0xca5...ee675 (blockchain)

- totalSupply
- symbol
- name
- decimals
- allowance address , address
- balanceOf address
- transferFrom address _from, address _to,
- burnFrom address _from, uint256 _val
- approve address _spender, uint256 _
- approveAndCall address _spender, uint256 _
- transfer address _to, uint256 _value
- burn uint256 _value

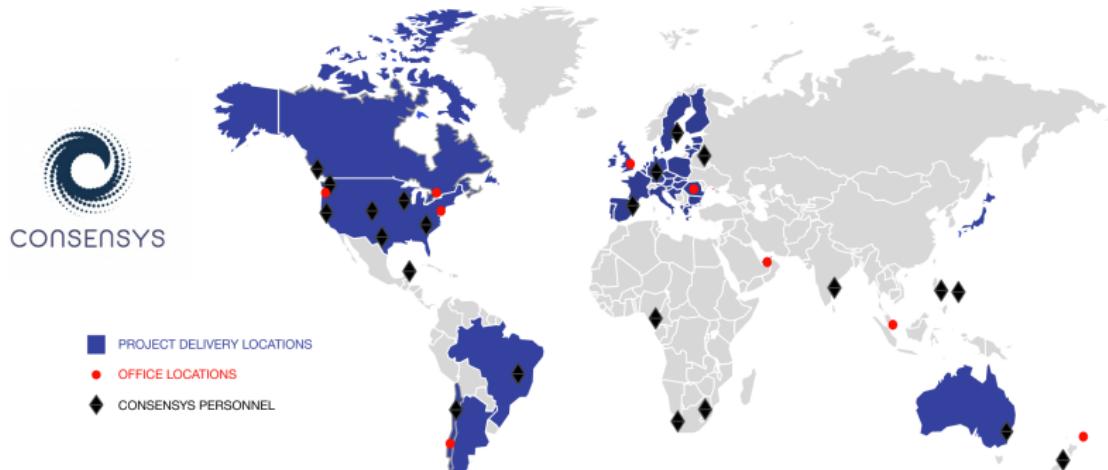


Table of Contents



The largest Blockchain Cie in the world

We are 1000+ blockchain experts, entrepreneurs, computer scientists, designers, engineers, consultants, and business leaders across 6 continents



Transforming Industries



ConsenSys partnered with a consortium of 15 key industry leaders and leading bank institutions to create a network-based commodities trading platform.



Transforming Industries



UNIONBANK

ConsenSys partnered with UnionBank to develop a closed-loop crypto-cash solution in the Philippines to connecting rural banks to the main financial infrastructure.

KALEIDO

A ConsenSys Business

Try it on  aws marketplace



Transforming Industries



mcCarthy
tetraul

ConsenSys has partnered with McCarthy-Tétrault to automate key aspects of the lending process by leveraging smart contract powered loan agreements on the Ethereum blockchain.

In this demo....



- OpenLaw's powerful markup language
- Digital, blockchain-based signatures
- Smart contract execution to a decentralized app ("dApp")



Fair Token Launches

The Brooklyn Project Framework

CIVIL Transparency Scorecard

as of 18 September 2018



Transparency Grading Scale

- 1 – 2 **Red flag** Non-existent or conflicting disclosures.
- 3 – 4 **Poor** Failure to reveal useful information.
- 5 – 6 **Lacking** Partially complete or unclear disclosures.
- 7 – 8 **Good** Standards met, but room for improvement.
- 9 – 10 **Very good** Complete, clear, consistent disclosures.

<https://framework.thebkp.com/project/CVL/document/2/version/3>

TOKEN FOUNDRY



<https://tokenfoundry.com/projects/civil>



Table of Contents



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum
- (March 14, 2016) Launch of Homestead, first production release



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum
- (March 14, 2016) Launch of Homestead, first production release
- (Spring 2016) The DAO



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum
- (March 14, 2016) Launch of Homestead, first production release
- (Spring 2016) The DAO
- (July 2, 2016) ETH – ETC split



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum
- (March 14, 2016) Launch of Homestead, first production release
- (Spring 2016) The DAO
- (July 2, 2016) ETH – ETC split
- (October 16, 2017) Launch of Metropolis (vByzantium) –version 3



A short history of Ethereum

Key Milestones:

- (late 2013) Vitalik Buterin describes Ethereum in a paper
- (Summer 2014) Ethereum raises more than \$14 million in pre-sale
- (July 30, 2015) Launch of Frontier, initial (beta) version of Ethereum
- (March 14, 2016) Launch of Homestead, first production release
- (Spring 2016) The DAO
- (July 2, 2016) ETH – ETC split
- (October 16, 2017) Launch of Metropolis (vByzantium) –version 3
- (2017) ETH goes from \$7 to more than \$700 (100x increase)

Check the nice infographic ([ethinfographic](#)).

More information:

- a “prehistory” of the Ethereum protocol ([vbuterin2017:prehistory](#)).
- the official *Ethereum White Paper*.



Decentralization

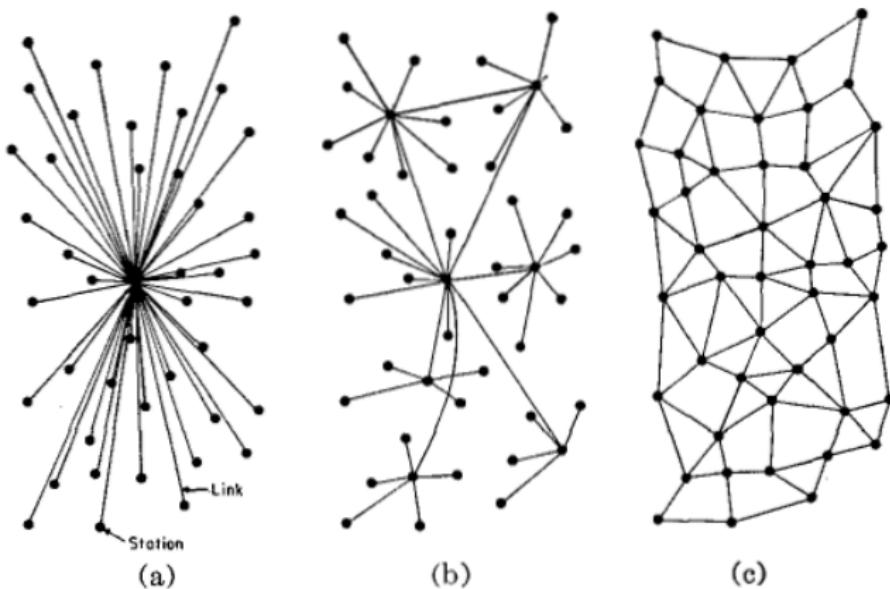


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.



Client Types

- Full node



Client Types

- Full node
- Light node



Client Types

- Full node
- Light node
- Something in between (e.g. “fast” for geth)



Disk Space

Full Archive Ethereum node

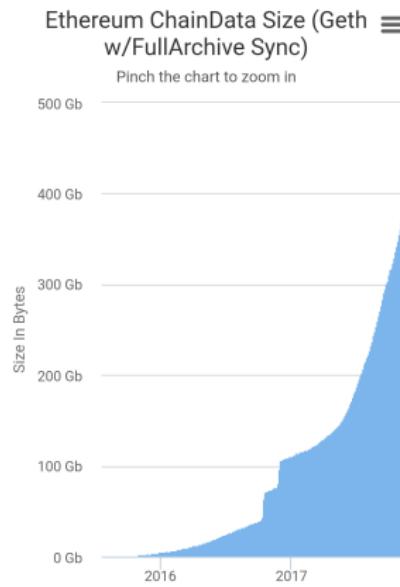


Figure: Miners need a lot of space ([reddit:chaindatasize](#))



Disk Space

Ethereum vs. Bitcoin

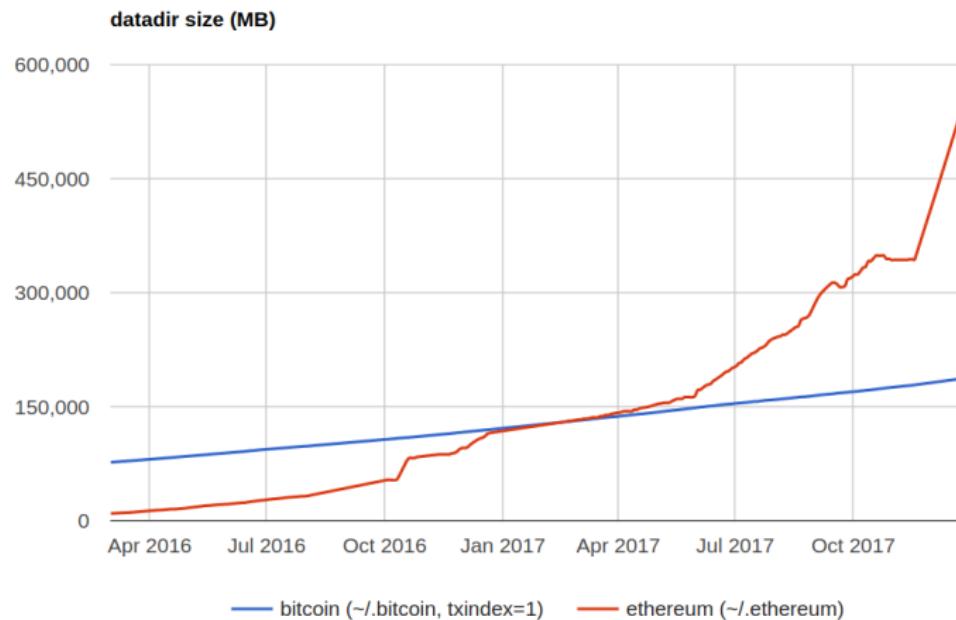


Figure: Disk space used by Geth (fast) vs. Bitcoin ([daniel:chaindatasize](#))

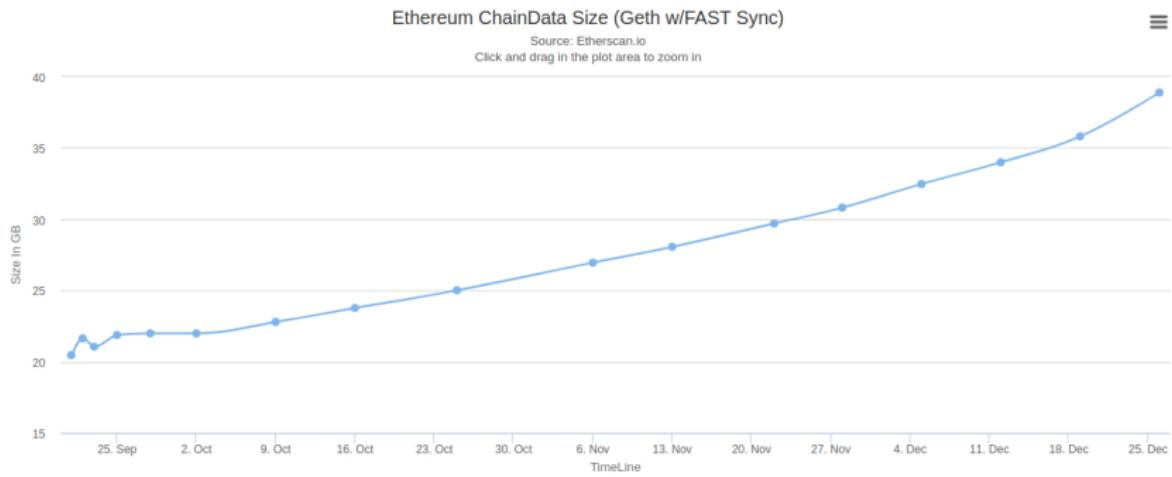


Disk Space

With Geth --syncmode fast (default mode)

This mode initializes a ~20 GB database, then turns in full node.

The GETH client has 3 Blockchain sync modes (fast, full or light). The 'FAST' sync was used to produce the data chart below using Geth v1.6.7 stable.



Disk Space

Parity allows for continuous state trie pruning

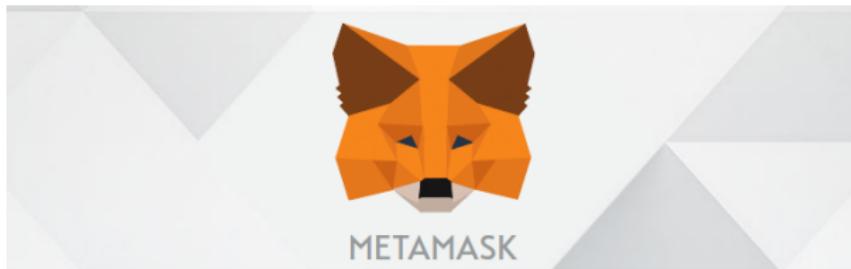
In green, the configuration running as *full node*.
A light client can fit in ~5 MB.

ID	Pruning Mode	Database Configuration	Block Verification	Available Blocks	Available States	Chaindata Size	Parity CLI Flags to use this configuration
0	Archive	+Fat +Trace	Full	All	All	385.000 GB	--pruning archive --tracing on --fat-db on
1	Archive	+Trace	Full	All	All	334.000 GB	--pruning archive --tracing on
2	Archive		Full	All	All	326.000 GB	--pruning archive
3	Fast	+Fat +Trace	Full	All	Recent	37.000 GB	--tracing on --fat-db on
4	Fast	+Trace	Full	All	Recent	34.000 GB	--tracing on
5	Fast		Full	All	Recent	26.000 GB	--no-warp
6	Fast	+Warp	Ancient-PoW-Only	All	Recent	25.000 GB	
7	Fast	+Warp -Ancient	No-Ancient	Recent	Recent	5.300 GB	--no-ancient-blocks
8	Light		Headers-Only	None	None	0.005 GB	--light

Figure: Disk space used by Parity (**afric:chaindatasize**)



Metamask



Brings Ethereum to your browser

[GET CHROME EXTENSION ►](#)

Chrome Firefox Opera

OR

[GET BRAVE BROWSER ►](#)

<https://metamask.io>



Practical Applications

for personal or business use

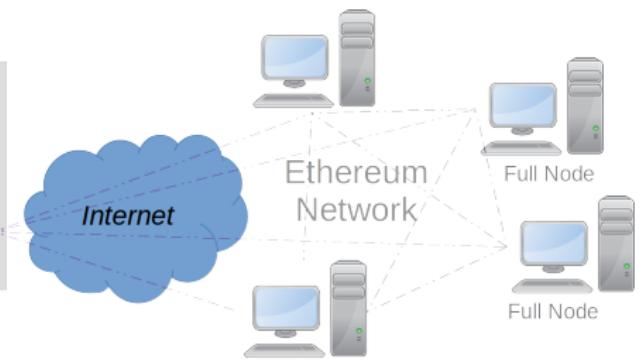
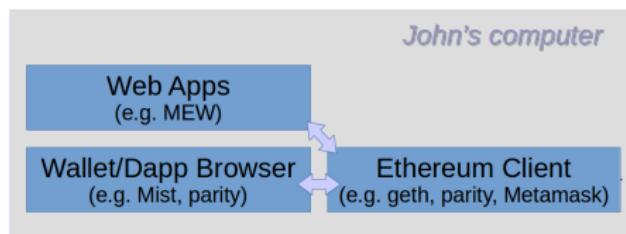


Table of Contents



Sizing up

- 1) Ethereum Node, Wallet, historical data, Smart Contracts, and Dapps:
 - Linux machine (Ubuntu 16.04 / Linux Mint 18.x –until April 2021)
 - Parity (or Geth)
 - A Solidity compiler
- 2) Developer light setup: (works on ChromeOS)
 - Chrome browser (or Chromium) –any OS
 - Metamask Extension
 - [Remix](#) IDE
- 3) Developer Pro setup:
 - [truffle](#)



Parity

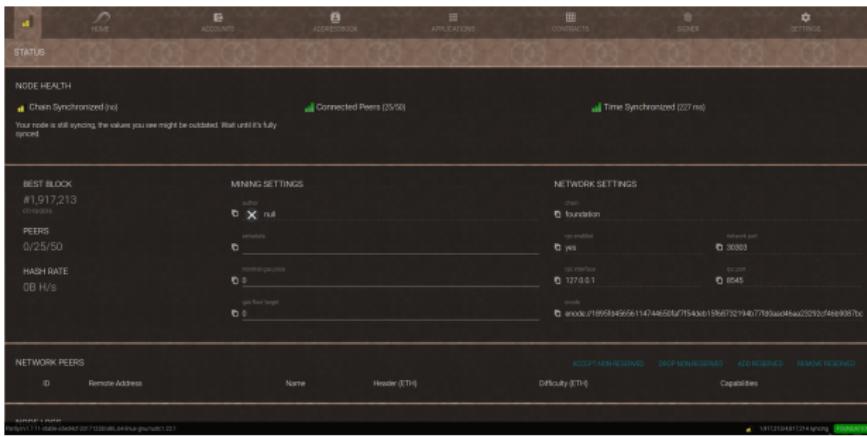


Figure: The Parity client syncing

- Typical Account Management, multi-sig, hardware support
 - Access Dapps directly (e.g. app to create an ERC-20 token)
 - Code editor and Solidity compiler for smart contracts
 - Fast and reliable (written in Rust)
 - Most OS, Docker images; and compliant with JSON-RPC API

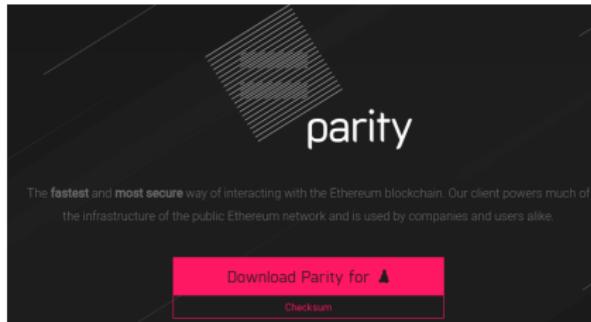


Lab 1: set up a full Development Environment

Installing Parity



Installing Parity



<https://www.youtube.com/watch?v=WNT2O6xyDmM> (Windows-based, 16 min)

- ① Go to <https://www.parity.io>
- ② Download the relevant binaries, e.g. on Linux:
- ③ Check the checksum: `$ md5sum parity_1.7.11_amd64.deb`
- ④ Install: `$ sudo dpkg -i parity_1.7.11_amd64.deb`
- ⑤ Check the version: `$ parity -v`



Run Parity on the Kovan Testnet

```
$ parity --light --testnet
2017-12-28 23:38:25 Starting Parity/v1.7.11-stable-a5ed4cf-20171228/x86_64-linux-gnu/rustc1.22.1
2017-12-28 23:38:25 Keys path /home/marc/.local/share/io.parity.ethereum/keys/Kovan
2017-12-28 23:38:25 DB path /home/marc/.local/share/io.parity.ethereum/chains/kovan/db/9bf388941c25ea98
2017-12-28 23:38:25 Path to dapps /home/marc/.local/share/io.parity.ethereum/dapps
2017-12-28 23:38:25 Running in experimental Light Client mode.
...
...
```

Then go to <http://localhost:8180> (or <http://web3.site> if online), and follow the instructions.

- After reading the legal terms and conditions, you can create your first account.
- Click on the top left-most logo (yellow bars) to see the status of your node.
- **It may take days to sync!**



Try running your first Dapp

Follow the tutorial at

<https://wiki.parity.io/Deploying-Dapps-to-Parity-Wallet> (using chevdor's dapp generator and yeoman)

On Linux Ubuntu, make sure you have npm, and make a soft link to node before running init.sh:

```
$ sudo apt install npm  
$ sudo ln -s /usr/bin/nodejs /usr/bin/node  
$ ./init.sh
```



Installing Geth



Installing Geth

Instructions (all OSes) at

<https://github.com/ethereum/go-ethereum/wiki/Building-Ethereum>.

Ubuntu/Mint: <https://github.com/ethereum/go-ethereum/wiki/Installation-Instructions-for-Ubuntu>

```
$ sudo apt-get install software-properties-common  
$ sudo add-apt-repository -y ppa:ethereum/ethereum  
$ sudo apt-get update
```

Run the first line to install the full suite (geth, bootnode, evm, disasm, rlpdump, ethtest), or the second line for geth only:

```
$ sudo apt-get install ethereum  
$ sudo apt-get install geth
```

Create a new account, and you should be ready to run geth:

```
$ geth account new  
$ geth
```



Installing a Solidity Compiler

Provided the previous steps were completed:

```
$ sudo apt-get install solc  
$ which solc
```

And in geth, to let it know where solc can be found:

```
$ admin.setSolc("/usr/bin/solc")
```

Now test the code by following the instructions at

<https://github.com/ethereum/go-ethereum/wiki/Contract-Tutorial>



Code Editor



- Vim
- Vim Solidity
- Vim Syntastic



And you still need a wallet

Options:

- Mist Browser (beta) (featured on the right, see also the recent security warning re. Chromium)
- MyEtherWallet (MEW) supports advanced features including hardware wallets

The screenshot shows the Mist Browser interface with the following details:

- Top navigation bar: WALLETS, SEND, CONTRACTS, BALANCE 0.00 ETHER.
- Peer status: 46,300 peers | 40,637,396 @ a minute since last block.
- Accounts Overview section:
 - ACCOUNTS: Main account (ETHERBASE) balance 0.00 ether.
 - WALLET CONTRACTS: No transactions yet.

Mist Browser (beta)
<https://wallet.ethereum.org>
Try on Chrome vs Firefox



Table of Contents

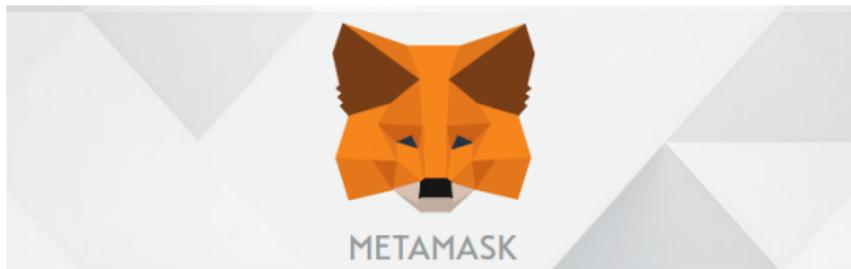


ConsenSys Dev Tools in Numbers

<https://www.youtube.com/watch?v=WKwR51ANy9E>



Metamask



Brings Ethereum to your browser

[GET CHROME EXTENSION ▶](#)

Chrome Firefox Opera

OR

[GET BRAVE BROWSER ▶](#)

<https://metamask.io>



Truffle Framework

<http://truffleframework.com>

YOUR ETHEREUM SWISS ARMY KNIFE

Truffle is the most popular development framework for Ethereum with a mission to make your life a whole lot easier.

Star 4,734

Fork 594

gitter [join chat](#)

INSTALL VIA NPM

```
$ npm install -g truffle
```

Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.

[DOCUMENTATION](#)

[TUTORIALS](#)

Don't know where to start? Get yourself a [Truffle Box!](#)



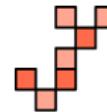
Infura

<http://infura.io>



BLOCKCHAIN BASED

We eliminate the need to install, configure, and maintain costly Ethereum infrastructure.



RELIABLE AND SCALABLE

Our Ferryman™ middleware improves reliability and helps us scale quickly to meet your demand.



DISTRIBUTED STORAGE

Access IPFS seamlessly without the hassle of managing the infrastructure.

POWERFUL AND SECURE

5B+

Requests Per Day

1.6PB

Data Transferred Per Month

9000+

Developers and DApps Served



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.

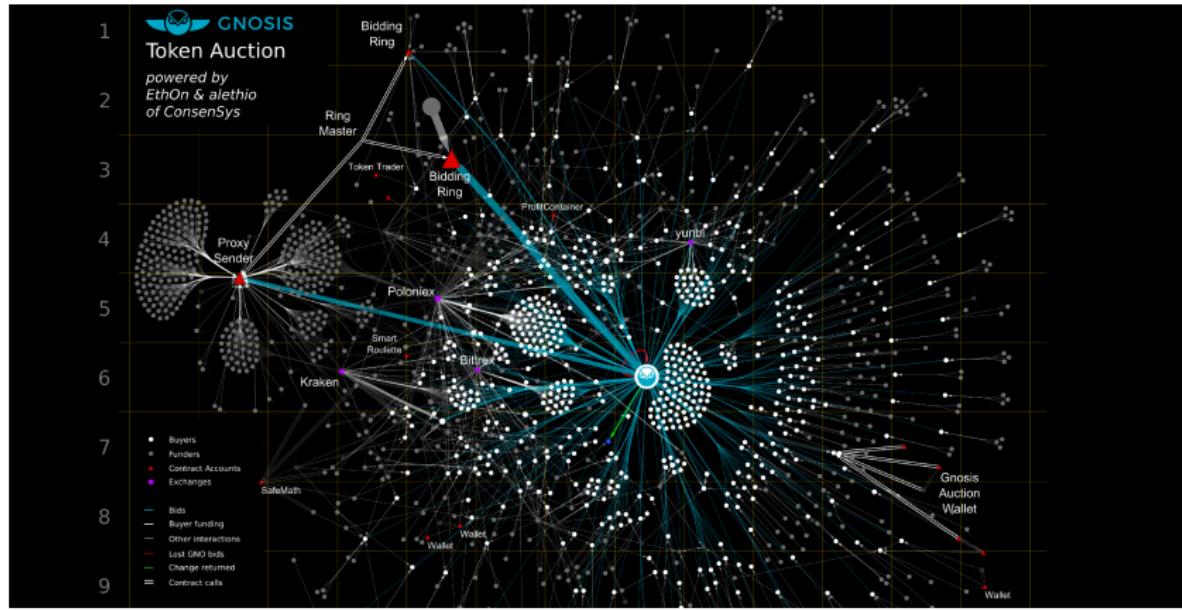
```
$ sudo apt install libssl-dev  
$ sudo apt install gcc g++  
$ sudo add-apt-repository ppa:ethereum/ethereum  
$ sudo apt install solc  
$ sudo pip3 install mythril  
$ myth -x contracts/higherbidder.sol
```

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



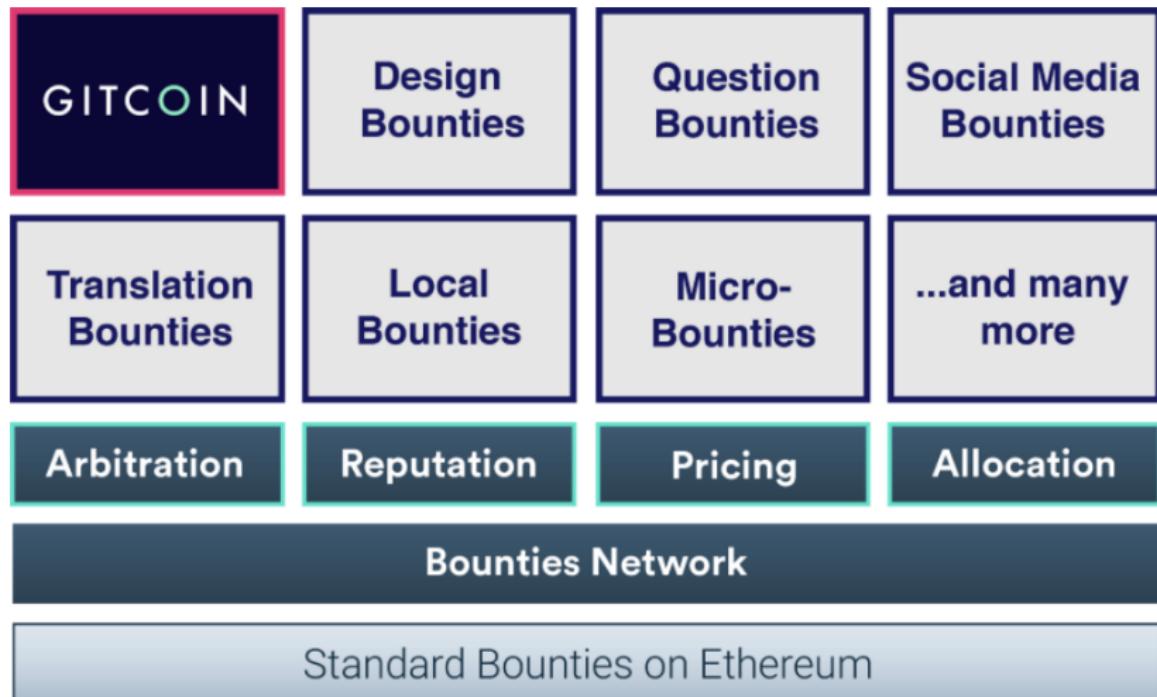
Big Data and Analytics on Ethereum

<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>

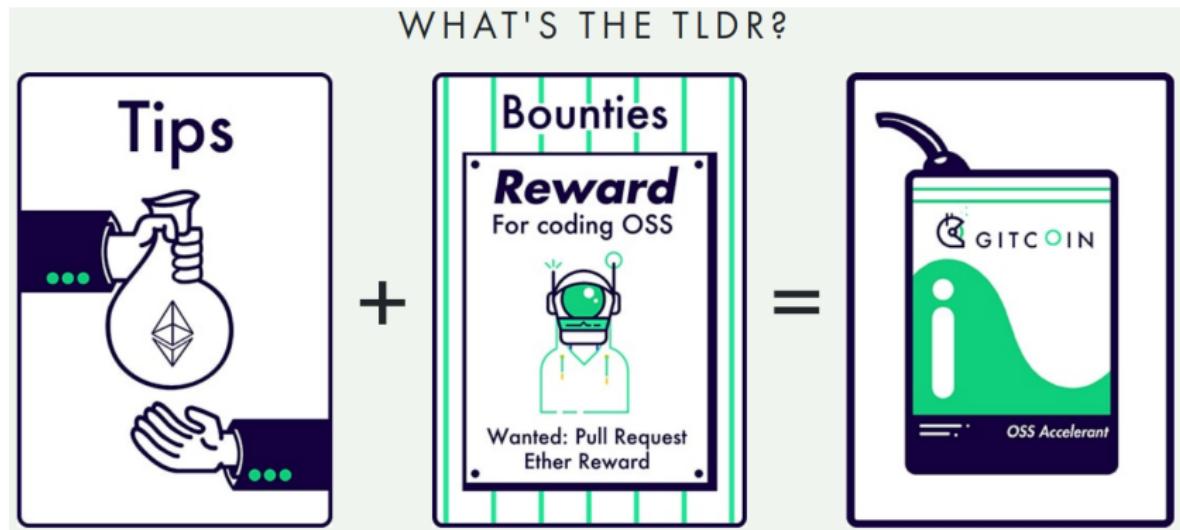


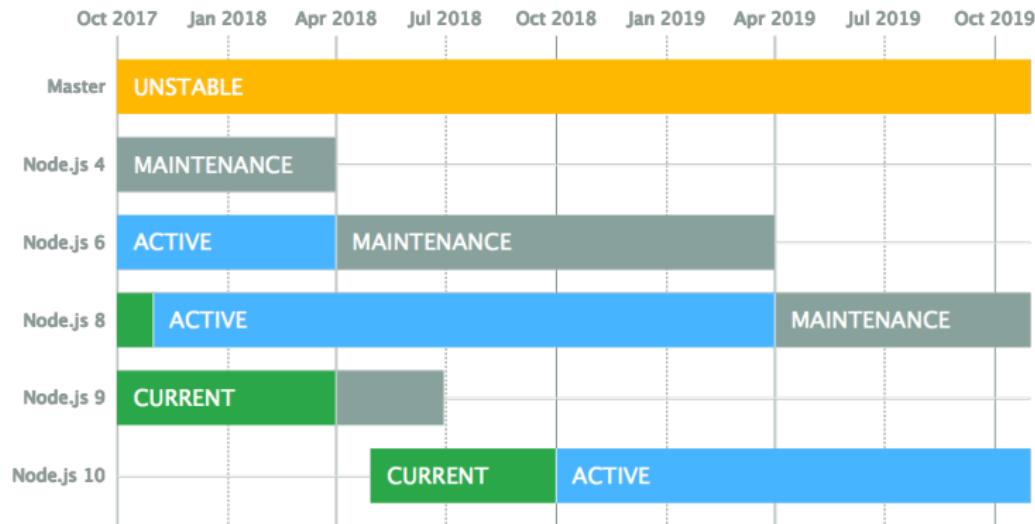
Table of Contents



Required dependency: node.js > 5

Install version 8 –in LTS maintenance until December 2019.

Run a script from <https://nodejs.org/en/download/package-manager/>



Installing Truffle

YOUR ETHEREUM SWISS ARMY KNIFE

Truffle is the most popular development framework for Ethereum with a mission to make your life a whole lot easier.



4,734



594



join chat

INSTALL VIA NPM

```
$ npm install -g truffle
```

Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.

DOCUMENTATION

TUTORIALS

Don't know where to start? Get yourself a [Truffle Box!](#)



Let's build our first Dapp with Truffle

<http://truffleframework.com/tutorials/pet-shop>



Let's build an ERC20 Token Contract with Truffle

[http://truffleframework.com/tutorials/
robust-smart-contracts-with-openzeppelin](http://truffleframework.com/tutorials/robust-smart-contracts-with-openzeppelin)



Table of Contents



Let's create our own
permission-based private
Blockchain
based on Ethereum!



Create a PoA chain with Parity

- PoA: Proof of Authority



Create a PoA chain with Parity

- PoA: Proof of Authority
- PoA is another type of consensus algorithm (not PoW), with no mining required



Create a PoA chain with Parity

- PoA: Proof of Authority
- PoA is another type of consensus algorithm (not PoW), with no mining required
- Less computationally intensive, more secure for small networks, faster



Create a PoA chain with Parity

- PoA: Proof of Authority
- PoA is another type of consensus algorithm (not PoW), with no mining required
- Less computationally intensive, more secure for small networks, faster
- The Kovan test network, Hyperledger and Ripple run on a PoA
- Parity supports two PoA consensus algorithm: Aura, and Tendermint (experimental)



Create a PoA chain with Parity

- PoA: Proof of Authority
- PoA is another type of consensus algorithm (not PoW), with no mining required
- Less computationally intensive, more secure for small networks, faster
- The Kovan test network, Hyperledger and Ripple run on a PoA
- Parity supports two PoA consensus algorithm: Aura, and Tendermint (experimental)
- Let's follow Parity's Demo PoA tutorial
- Simple Hands-on at
<https://github.com/marclijour/parity-poa-tutorial>



Parity's Demo PoA tutorial

Objectives:

- ① Setup two connected nodes on one machine (for demo)
- ② Gain familiarity with Parity (UI and command line)
- ③ Gain a better understanding of diverse types of blockchain (public/private, permissionless/permission-based) and different types of consensus algorithms



Parity's Demo PoA tutorial

Step 1: download the files

This [tutorial](#) assumes than you have installed Parity. Instructions are shown for a machine running Linux Ubuntu. The first step consists in cloning the GitHub repo in your machine. You'll run command from within that directory.

```
$ git clone https://github.com/marclijour/parity-poa-tutorial.git
```



Parity's Demo PoA tutorial

Step 2: create nodes and accounts

From the “parity-poa-tutorial” directory, open two terminals and type one line in each:

```
$ parity --config node0.starthere  
$ parity --config node1.starthere
```

Open another console and run these scripts:

```
$ ./create_first_authority_address_on_node0.sh  
$ ./create_second_authority_address_on_node1.sh  
$ ./create_user__address_on_node0.sh
```



Parity's Demo PoA tutorial

Step 3: start the chain on PoA

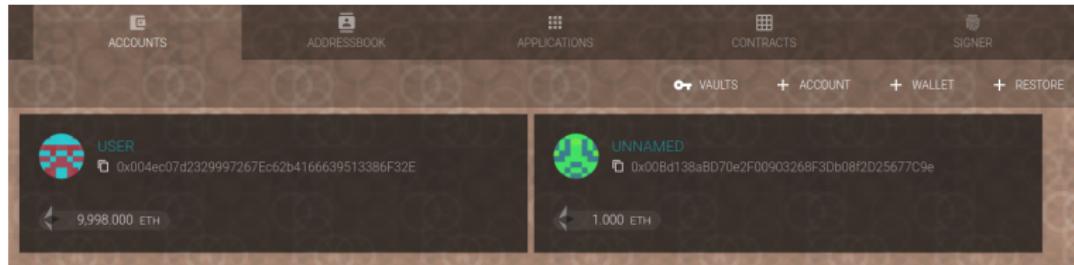
In two separate terminals, restart parity with this new configuration.

```
$ parity --config node0.toml  
$ parity --config node1.toml
```



Parity's Demo PoA tutorial – Step 4: setup the Parity UI

Open two different windows or tabs in your browser for node 0 (at <http://localhost:8181>) and node 1 (at <http://localhost:8182>).



Restore the accounts as above:

- on node 0: node0 (password = node0), and user (password = user)
- on node 1: node1 (password = node1)



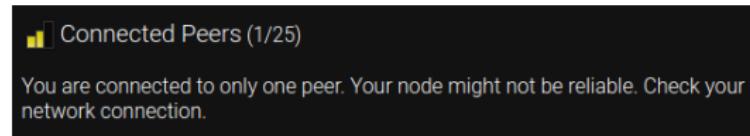
Parity's Demo PoA tutorial

Step 4: connect the nodes with each other

Check the console where you started node 0, and look for the Public Node URL. It should resemble something like this: `enode://<long hash>@<IP Address>:<Port Number>`

NETWORK PEERS				ACCEPT NON RESERVED	DROP NON RESERVED	ADD RESERVED	REMOVE RESERVED
ID	Remote Address	Name		Header (ETH)	Difficulty (ETH)	Capabilities	
1	75723705b1b77fe6b7	192.168.0.16:30301	Parity/v1.7.11-stable-5fed4cf-20171228@86.64.lnux-gnu/rustc1.22.1	0x0993...fd1ed1	2.0757224082177246e+40	eth/v6 - eth/v3 - parity/v2 - pip/v1	

Go to the Status tab (the leftmost tab) in the Web UI for node 1, and look for the Network Peers section. Click on ADD RESERVED, and copy the URL (including `enode://`).



Check the console output and the Web UI. Both should acknowledge another peer (1/25 Peers instead of 0/25 Peers).



Parity's Demo PoA tutorial

Step 5: send transactions

Run the following scripts and watch the balance for each account in the Web UIs.

```
$ send_from_user_to_node0_account.sh  
$ send_from_user_to_node1_account.sh
```

You can also try in a separate console, where you can read the JSON-formatted response.

```
$check_balance_in_node0_account.sh  
$check_balance_in_node1_account.sh
```



Parity's Demo PoA tutorial

Step 6: add nodes to the network

Run parity with the right chain specification and let other nodes know (by adding them by enode URL). You just need the demo-spec.json file to get started.

```
$ parity --chain demo-spec.json
```



It's the beginning of a
rewarding journey...



Next Steps and Recommended Readings

- Starting on Blockchain: key learning resources
- Fairly exhaustive references from Andreessen Horowitz
- Parity Wiki (e.g. Token Deployment)
- Ethereum White Paper and Wiki
- MOOCs: Udemy (Solidity), edX (Hyperledger)
- Building Blockchain Projects: Building decentralized Blockchain applications with Ethereum and Solidity by Narayan Prusty (2017)
-check the section on Proof of Authority (PoA)



Thank you!

Email: marc@lijour.net

Twitter: [@marclijour](https://twitter.com/marclijour)



References

