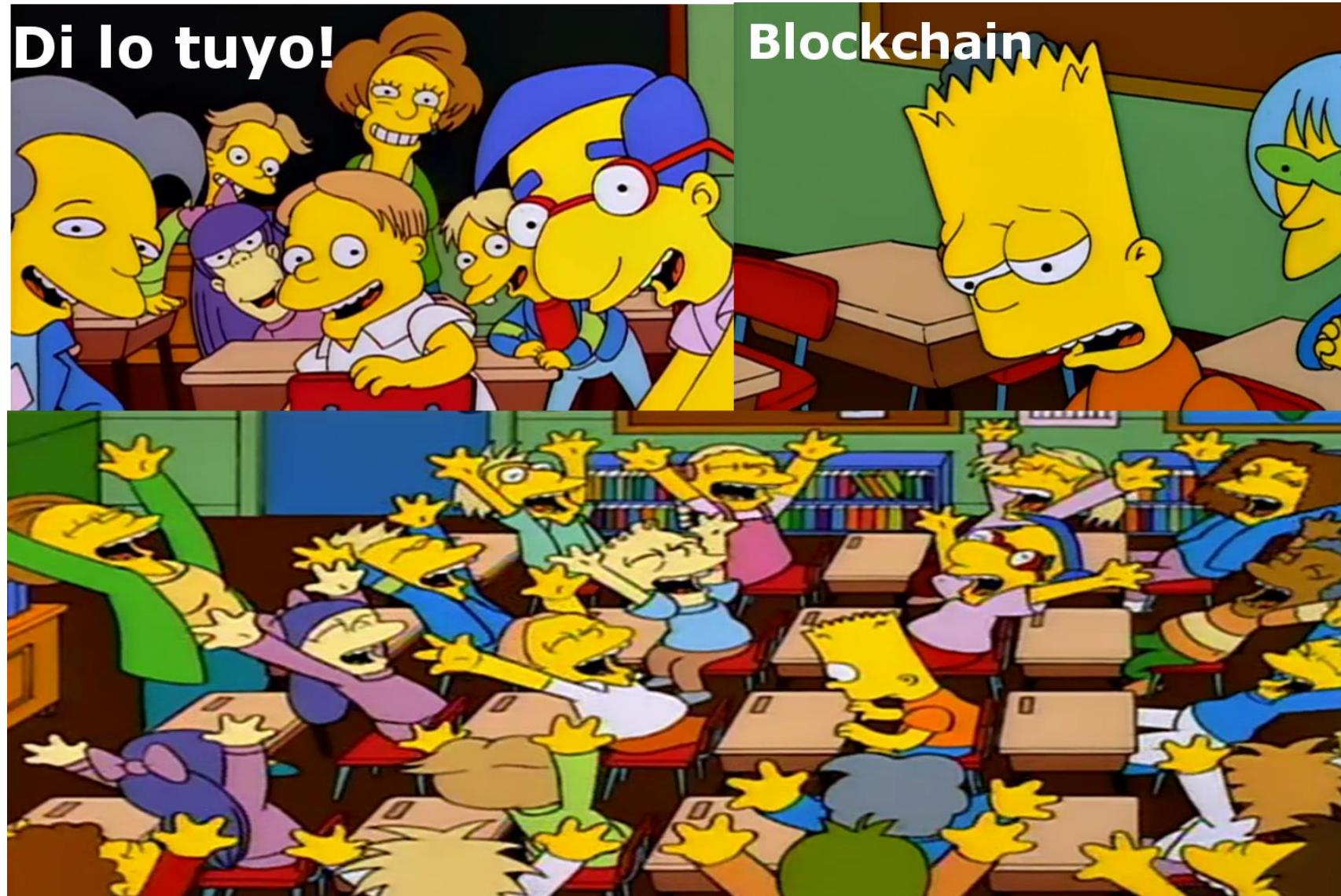


Development for Blockchain + Decentralized Applications



State of Blockchain



State of Blockchain

2017

Company's name changes to:
Long Blockchain Corp.



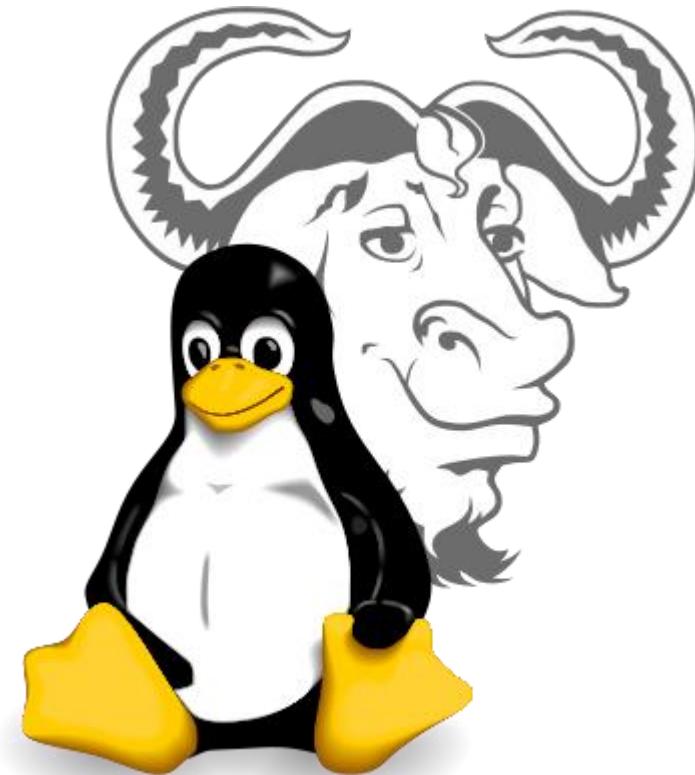
YOUR MONEY

TEA COMPANY GETS IN ON BITCOIN CRAZE

8:18 ET

HLN

State of Blockchain



#whoami

Web/Mobile Developer

Systems Engineer

(Scholarship 2010 Navarra Public University)

Master Security Informatics

(Scholarship 2016 Salamanca University)

Email: vicsanjinez@gmail.com

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

Github: <https://github.com/vicsanjinez>

Linkedin: <https://www.linkedin.com/in/victor-sanjinez-78484170/>



Disclaimer

All the content of this talk is
just for academic or legal
activities



Disclaimer

Marco Legal



Artículo 331 de la Constitución Política del Estado

La prestación de servicios financieros y cualquier otra actividad relacionada con el manejo, aprovechamiento e inversión del ahorro, son de interés público y solo pueden ser ejercidas previa autorización del Estado

Ley N° 393 de Servicios Financieros, a través del Artículo 491 incorpora al Código Penal

La intermediación financiera sin autorización o licencia, es un delito de orden público con una pena de privación de libertad de (5) cinco a (10) diez años y multa de (100) cien a (500) quinientos días.

Disclaimer

Banco Central de Bolivia [BO] | https://www.bcb.gob.bo/webdocs/11_comunicados/04_2017_COMUNICADO_Uso_monedas.pdf

04_2017_COMUNICADO_Uso_monedas.pdf 1 / 1



BANCO CENTRAL DE BOLIVIA
ESTADO PLURINACIONAL DE BOLIVIA

COMUNICADO 04/2017

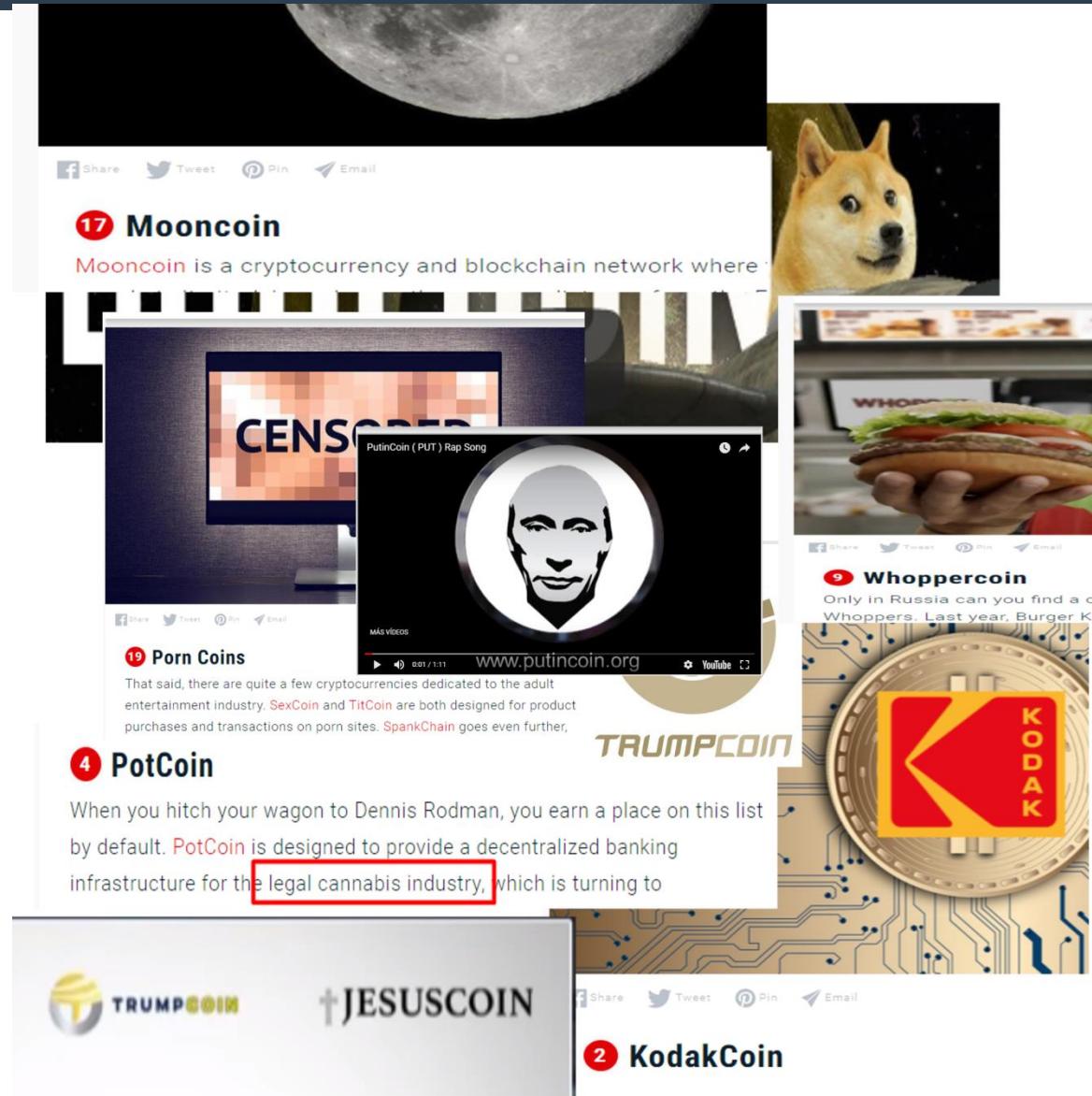
El Banco Central de Bolivia – BCB recuerda a la población en general que está prohibido el uso de monedas no emitidas o reguladas por países o zonas económicas así como el procesamiento de órdenes electrónicas de pago en monedas y denominaciones monetarias no autorizadas por el BCB en el ámbito del sistema de pagos nacional, de acuerdo a lo establecido en la Resolución de Directorio N°044/2014 de 06.05.2014.

Las denominadas monedas virtuales, que no son emitidas por estados o bancos centrales, no cumplen con todas las funciones económicas del dinero como medio de pago, unidad de cuenta y depósito de valor.

El uso y emisión de monedas virtuales como el Bitcoin, Namecoin, Tonal Bitcoin, IxCoin, Devcoin, Freicoin, 10coin, Liquidcoin, Peercoin, Quark, Primecoin, Feathercoin y otras que no pertenecen a ningún país o zona económica, no está regulado, se desconoce su origen y en consecuencia podrían ocasionar pérdidas a sus tenedores.

La Paz, abril de 2017

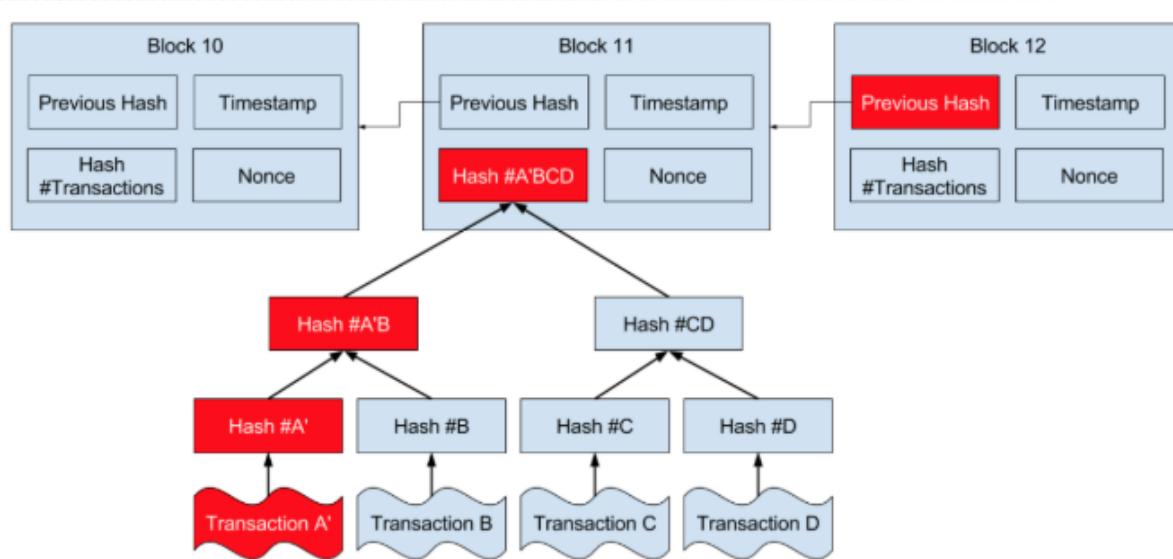
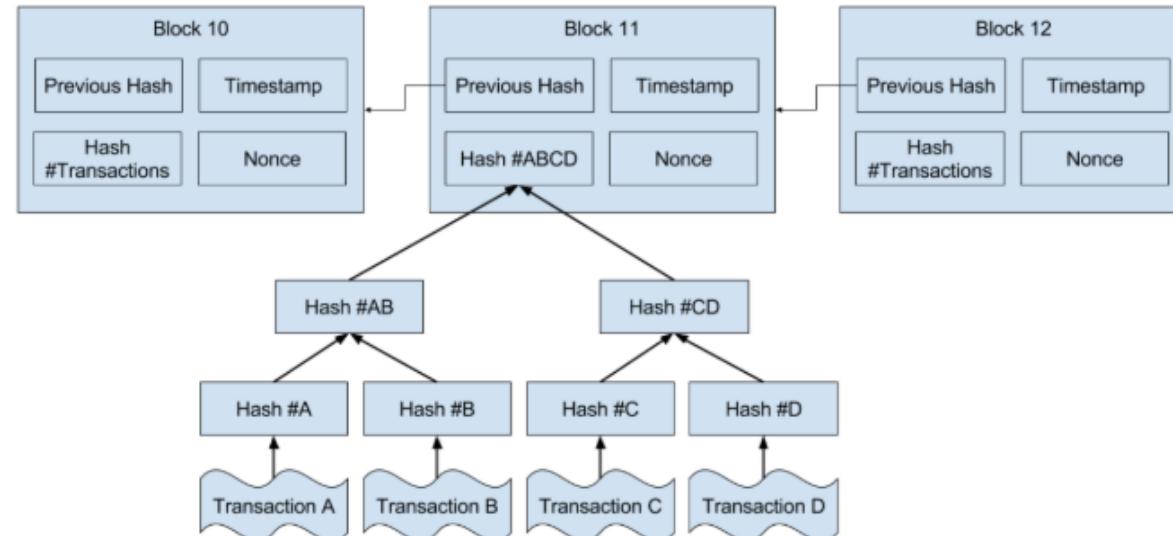
Disclaimer



What is Blockchain?

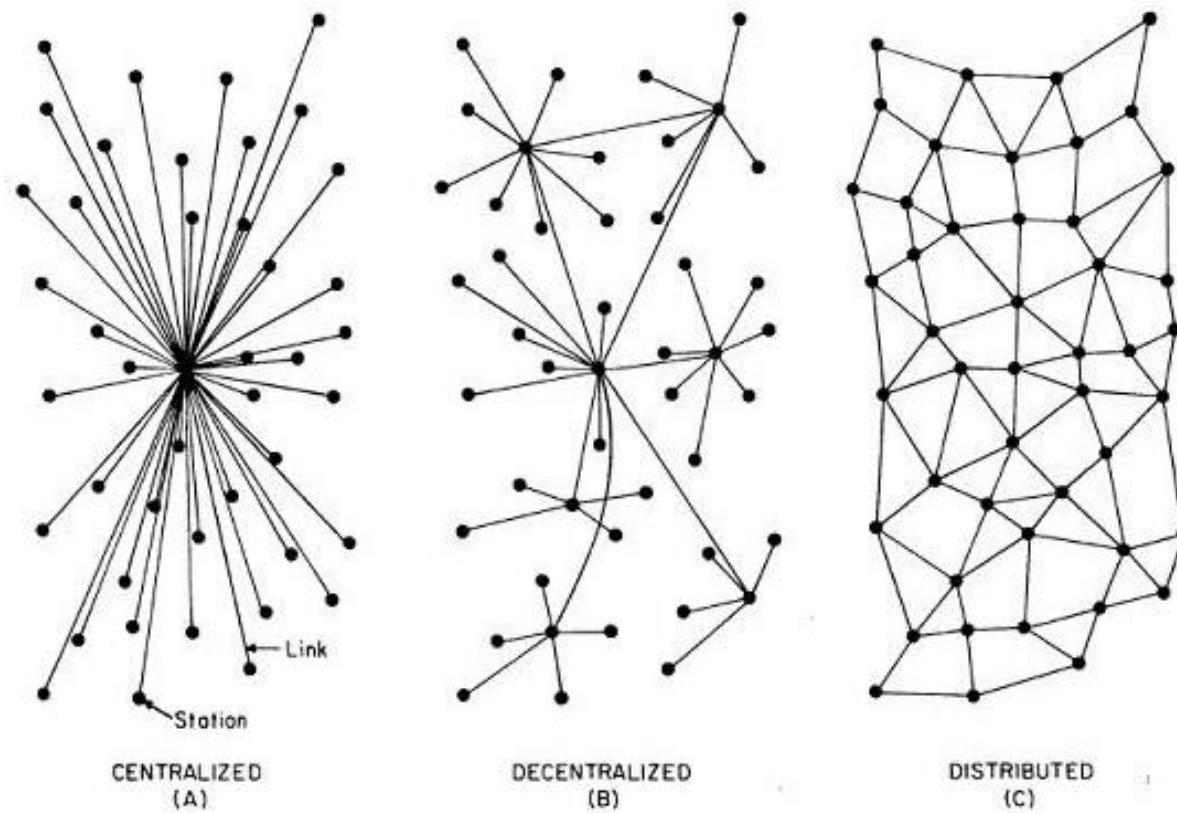
Blockchain
is a set of **Transactions**
grouped in **Blocks**
where each Block has a **Hash**
that is used as the **Start of the Next Block**
and all this happens in a **Decentralized**
environment

What is Blockchain?

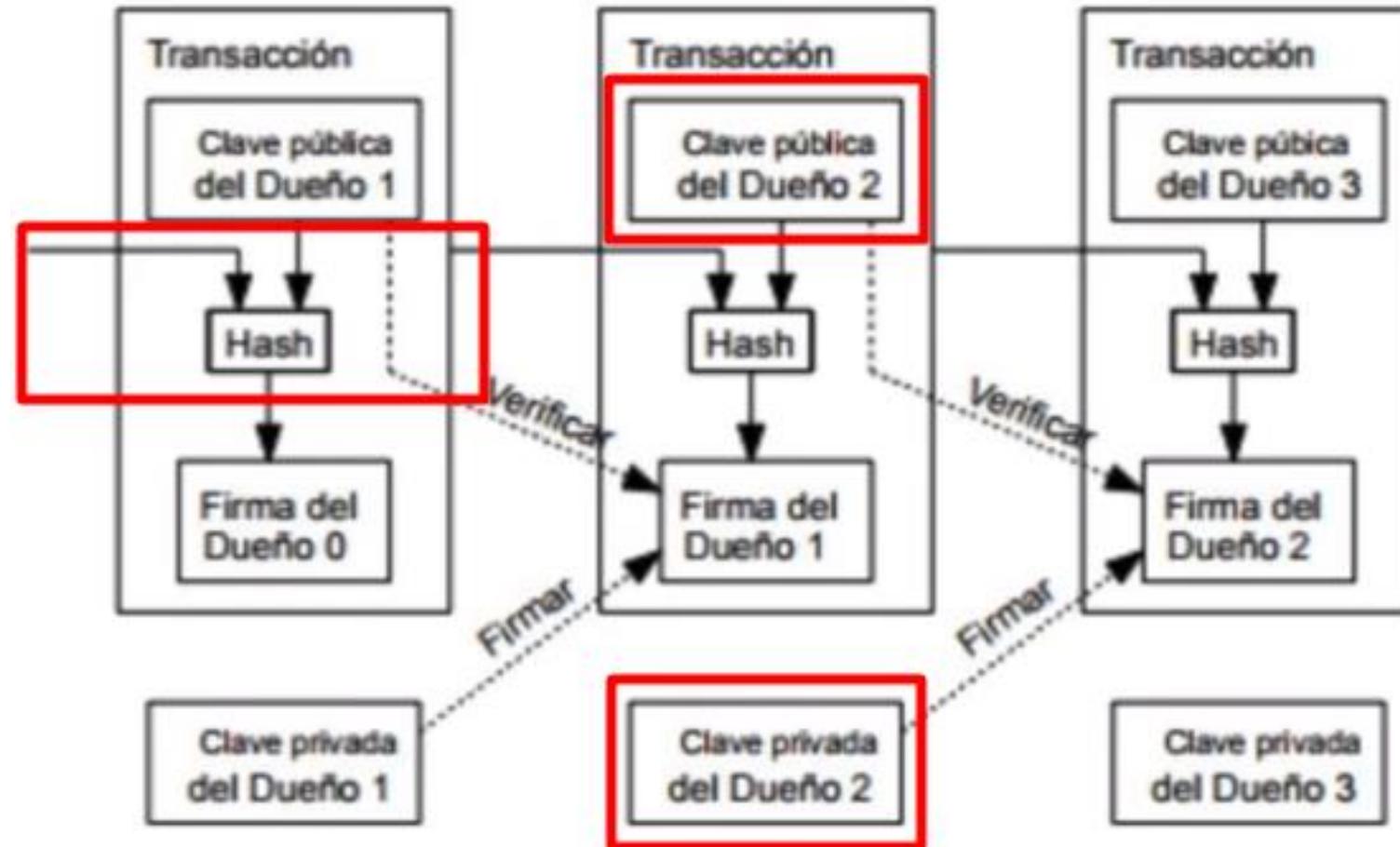


Benefits of Blockchain: Decentralized

Decentralized vs Centralized vs Distributed. What's the difference?



Benefits of Blockchain: Integrity (Hash and Public and Private Keys)



Benefits of Blockchain: Integrity (New Block)

```
#      @data="Hello, Cryptos!",
#      @hash="00ecb8b247998f9ddd15d2a5693777ee0041d138fa3bc5c1f6ccc12ec1cfce4",
#      @nonce=143>
#
#      pp Block.new( 'Hello, Cryptos! - Hello, Cryptos! - Hello, Cryptos!' )
#=> #<Block:0x1d67f18
#      @data="Hello, Cryptos! - Hello, Cryptos! - Hello, Cryptos!",
#      @hash="0014406a868d202e2c6c3896af997e189daafc9df1878f9824cba2050fda199f",
#      @nonce=59>
#
#      pp Block.new( 'Your Name Here' )
#=> #<Block:0x1d64270
#      @data="Your Name Here",
#      @hash="0012c3a90e58c9569ef0c036e6220c86c7c253ac94c0eb0064bf98df59acdfad",
#      @nonce=57>
#
#      pp Block.new( 'Data Data Data Data' )
#=> #<Block:0x139b828
#      @data="Data Data Data Data",
#      @hash="00e2da510b97434713d63234f3ba2d816c8d52f29f9ffd267423c39d9ced7a70",
#      @nonce=73>
```

See the difference? Now all hashes start with '00' e.g.

Block	Hash with Proof-of-Work
#1	00ecb8b247998f9ddd15d2a5693777ee0041d138fa3bc5c1f6ccc12ec1cfce4
#2	0014406a868d202e2c6c3896af997e189daafc9df1878f9824cba2050fda199f
#3	0012c3a90e58c9569ef0c036e6220c86c7c253ac94c0eb0064bf98df59acdfad
#4	00e2da510b97434713d63234f3ba2d816c8d52f29f9ffd267423c39d9ced7a70

History



History

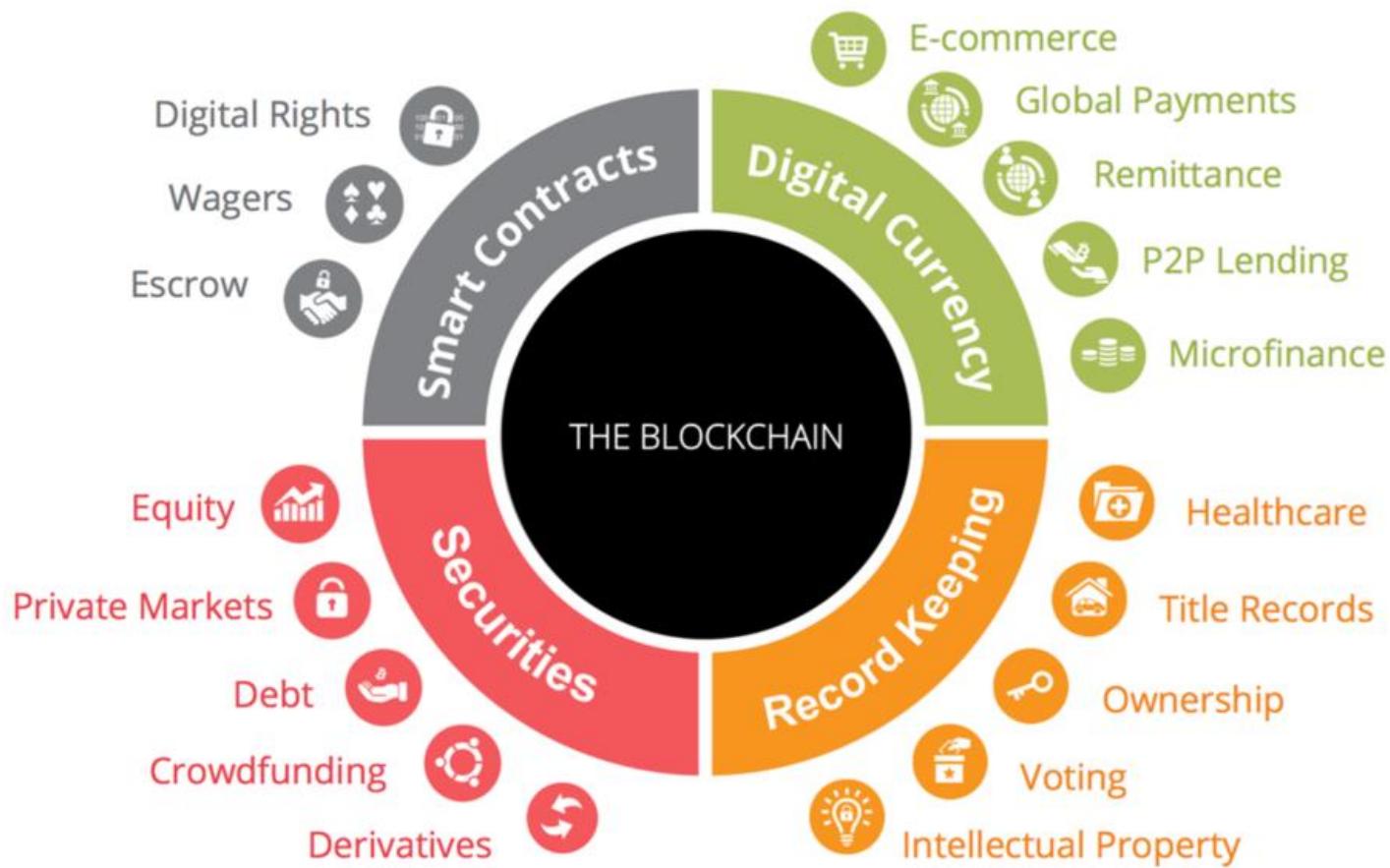
Breve historia del Bitcoin

-
- The timeline consists of four yellow chevron-shaped boxes pointing downwards, each containing a year and a corresponding historical event. The years are 2008, 2009, 2010, and 2011. The events are: 2008 - Publicación de un artículo científico/técnico sobre un sistema descentralizado que permitiría la emision de una criptomonedera. 2009 - Reserva del dominio bitcoin.org, Inserción del primer bloque de Bitcoin (Genesis). 2010 - Se compra la primera pizza en bitcoins. 2 pizzas por 10.000 Bitcoins (1). 2011 - Se alcanza la paridad Bitcoin / Dollar.
- 2008** Publicación de un artículo científico/técnico sobre un sistema descentralizado que permitiría la emisión de una criptomonedera.
 - 2009** Reserva del dominio bitcoin.org
Inserción del primer bloque de Bitcoin (Genesis)
 - 2010** Se compra la primera pizza en bitcoins. 2 pizzas por 10.000 Bitcoins (1)
 - 2011** Se alcanza la paridad Bitcoin / Dollar

Projects for Blockchain (Bored)

Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries



Projects for Blockchain (Awesome)

www.youtube.com/results?search_query=blockchain&sp=CANCBAgBEgA%253D

blockchain

Blockchain is Eating Wall Street | Alex Tapscott | TEDxSanFrancisco
TEDx Talks 627 mil visualizaciones • Hace 1 año

Author of best seller "blockchain revolution", Alex share in this talk about how the blockchain the technology behind bitcoin is ...

18:45

What Is Blockchain?
World Economic Forum 611 mil visualizaciones • Hace 2 años

By using math and cryptography, Blockchain is challenging the status quo in a radical way. Will governments and financial ...

2:20

Why people are buying cartoon cats on the blockchain
Vox 601 mil visualizaciones • Hace 2 meses

Forget cryptocurrencies. These are cryptocollectibles. Subscribe to our channel! http://goo.gl/0bsAjO
Every time you send ...

Subtítulos

3:35

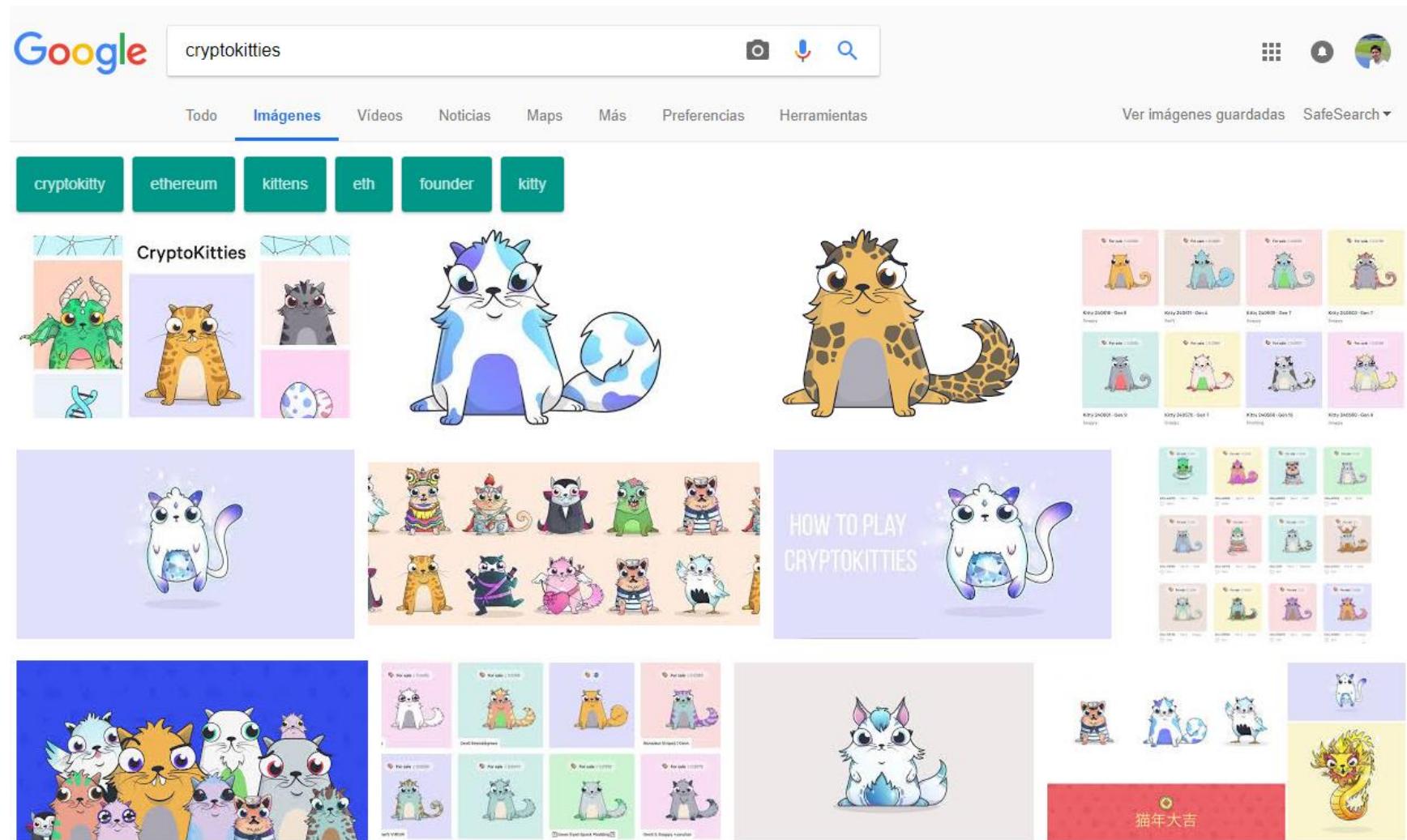
How it Works: Blockchain
IBM Think Academy 534 mil visualizaciones • Hace 1 año

Learn more about how blockchain works and see it in action within the diamond industry, which has been plagued by fraud, theft ...

EOS.IO: Why Blockchain?
EOS.IO 441 mil visualizaciones • Hace 5 meses

CTO Daniel Larimer and CEO Brendon Blumer from block.one share their thoughts on why the world

Projects for Blockchain (Awesome)



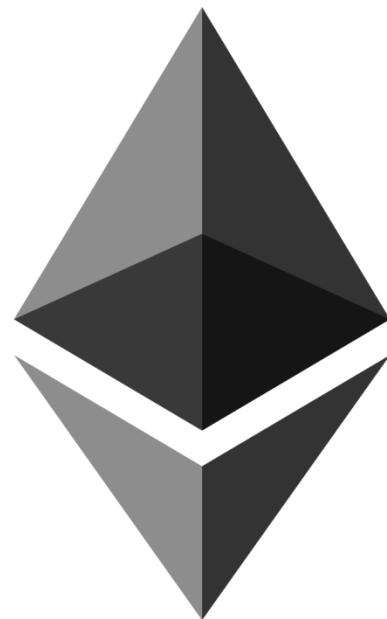
How develop for Blockchain?



Develop for Blockchain is easy!



Ethereum



etherium



Ethereum



ethereum



Smart Contracts



Solidity

```
1 pragma solidity ^0.4.19;
2
3 contract ZombieFactory {
4
5     // declare our event here
6     event NewZombie(uint zombieId, string name, uint dna);
7
8     uint dnaDigits = 16;
9     uint dnaModulus = 10 ** dnaDigits;
10
11    struct Zombie {
12        string name;
13        uint dna;
14    }
15
16    Zombie[] public zombies;
17
18    function _createZombie(string _name, uint _dna) private {
19        uint id = zombies.push(Zombie(_name, _dna)) - 1;
20        // and fire it here
21        NewZombie(id, _name, _dna);
22    }
23
24    function _generateRandomDna(string _str) private view returns (uint) {
25        uint rand = uint(keccak256(_str));
26        return rand % dnaModulus;
27    }
28
29    function createRandomZombie(string _name) public {
30        uint randDna = _generateRandomDna(_name);
31        _createZombie(_name, randDna);
32    }
33
34 }
35 }
```

Truffle



TRUFFLE



Ganache



Ganache

ONE CLICK BLOCKCHAIN

Quickly fire up a personal Ethereum blockchain which you can use to run tests, execute commands, and inspect state while controlling how the chain operates.

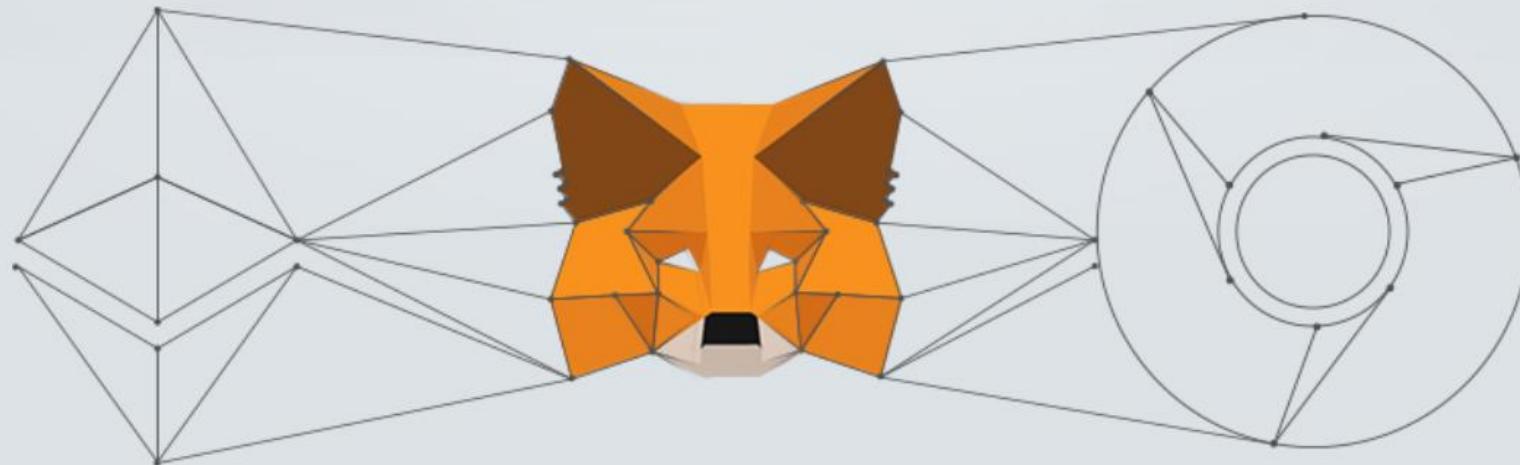
DOWNLOAD
(WINDOWS)



Need another OS download?



Metamask



MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.

MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.

You can install the MetaMask add-on in Chrome, Firefox, Opera, and the new [Brave browser](#). If you're a developer, you can [start developing with MetaMask today](#).

Our mission is to make Ethereum as easy to use for as many people as possible.

Demo



**KEEP
CALM
IT IS
DEMO
TIME**



Demo

windows7dapps (maquina-limpia) [Corriendo] - Oracle VM VirtualBox

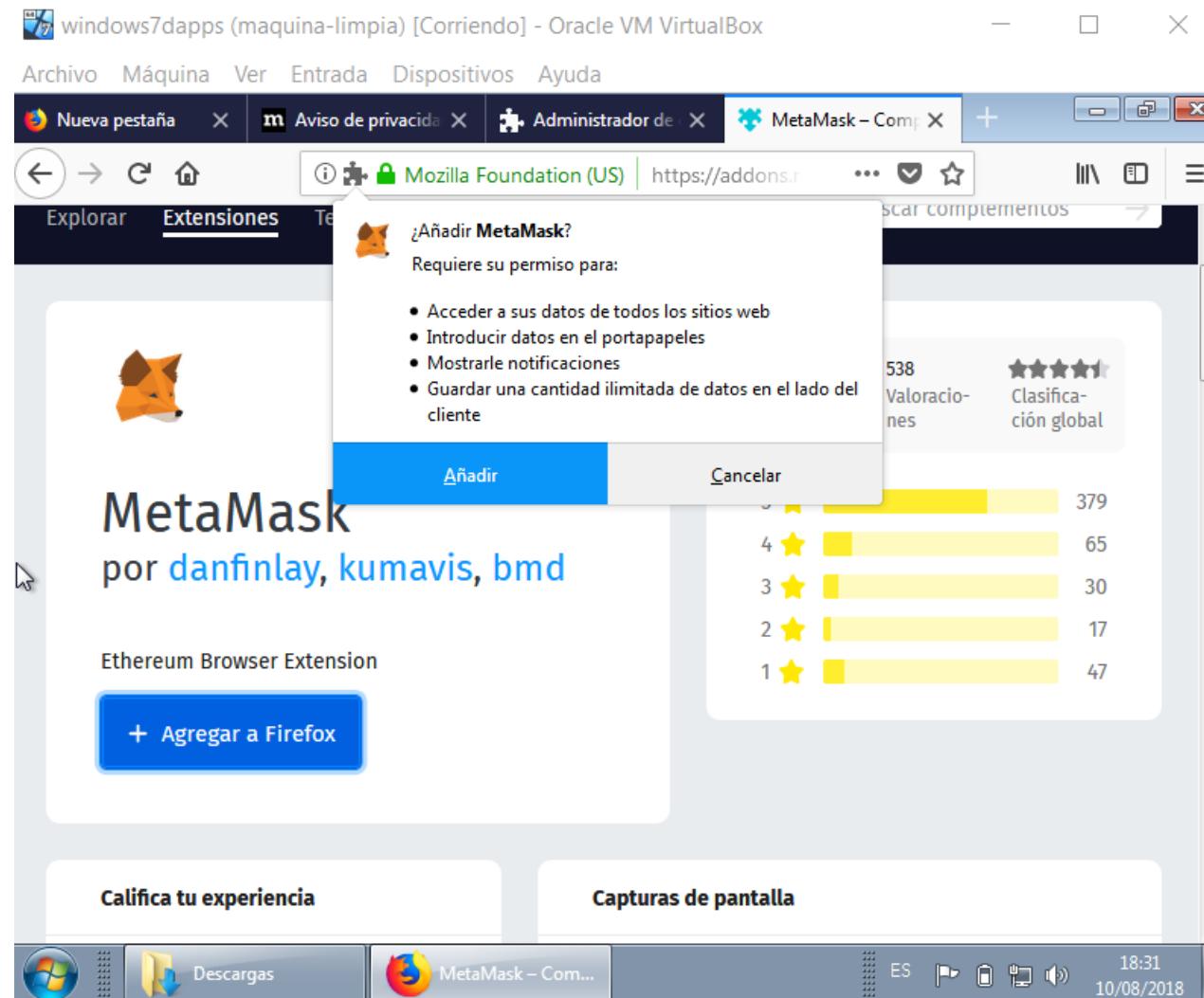
Archivo Máquina Ver Entrada Dispositivos Ayuda

Organizar Incluir en biblioteca Compartir con Nueva carpeta

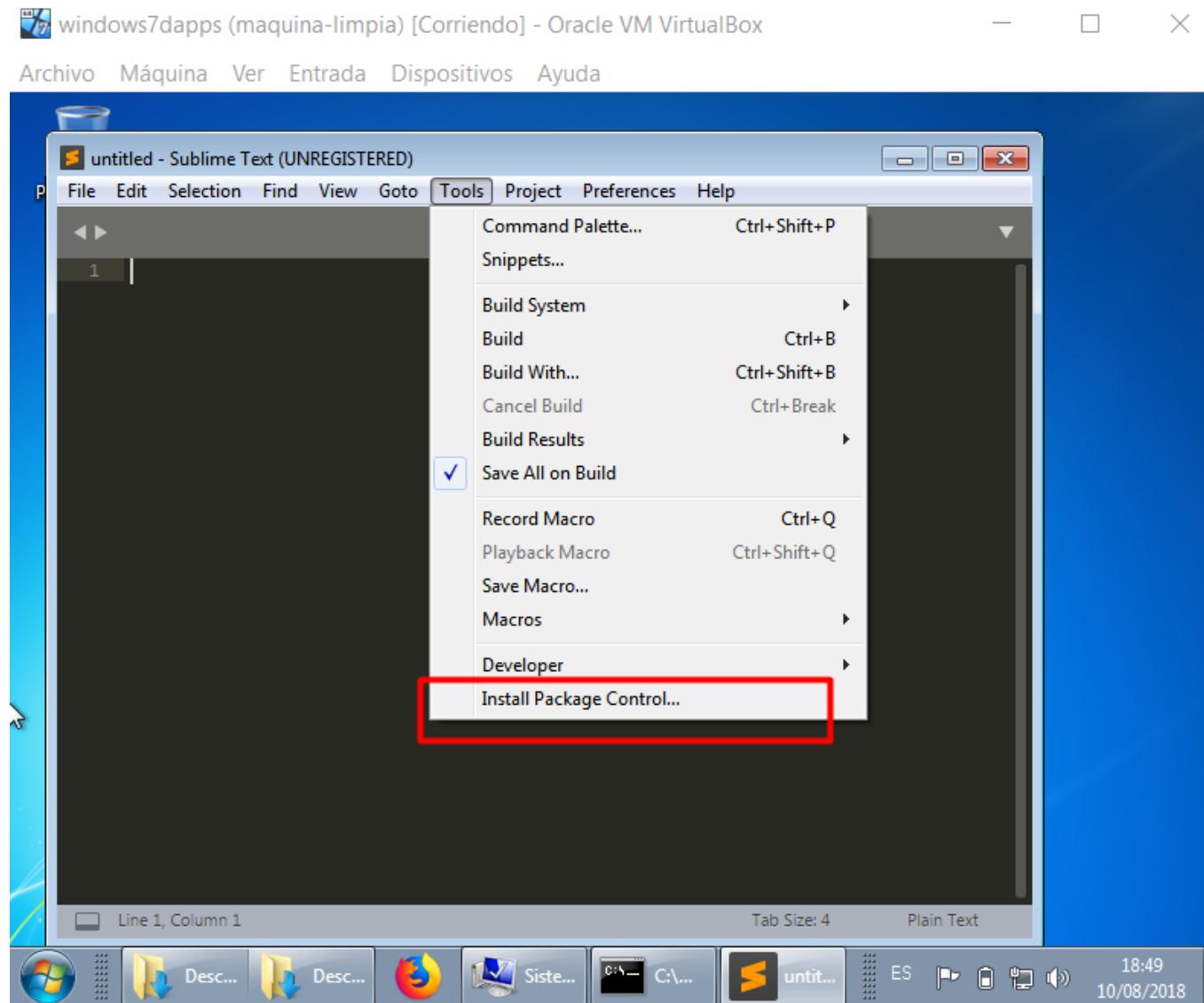
Buscar Descargas

Favoritos	Nombre	Fecha de modifica...	Tipo	Tamaño
Descargas	bitnami-wampstack-5.6.33-2-windows-x...	10/08/2018 18:23	Aplicación	182.376 KB
Escritorio	Composer-Setup	10/08/2018 18:21	Aplicación	748 KB
Sitios recientes	Firefox Installer	10/08/2018 18:21	Aplicación	307 KB
Bibliotecas	FoxitReader901_L10N_Setup_Prom	10/08/2018 18:22	Aplicación	75.607 KB
Documentos	ganache-setup-1.2.1	10/08/2018 18:23	Aplicación	113.403 KB
Imágenes	go-ipfs_v0.4.17_windows-amd64	10/08/2018 18:25	Carpeta comprimi...	9.928 KB
Música	node-v10.7.0-x64	10/08/2018 18:27	Paquete de Windo...	17.036 KB
Vídeos	npp.7.5.5.Installer.x64	10/08/2018 18:26	Aplicación	4.513 KB
Gráfico en el hogar	Sublime Text Build 3143 x64 Setup	10/08/2018 18:22	Aplicación	8.744 KB
	winrar-x64-550es	10/08/2018 18:25	Aplicación	2.266 KB

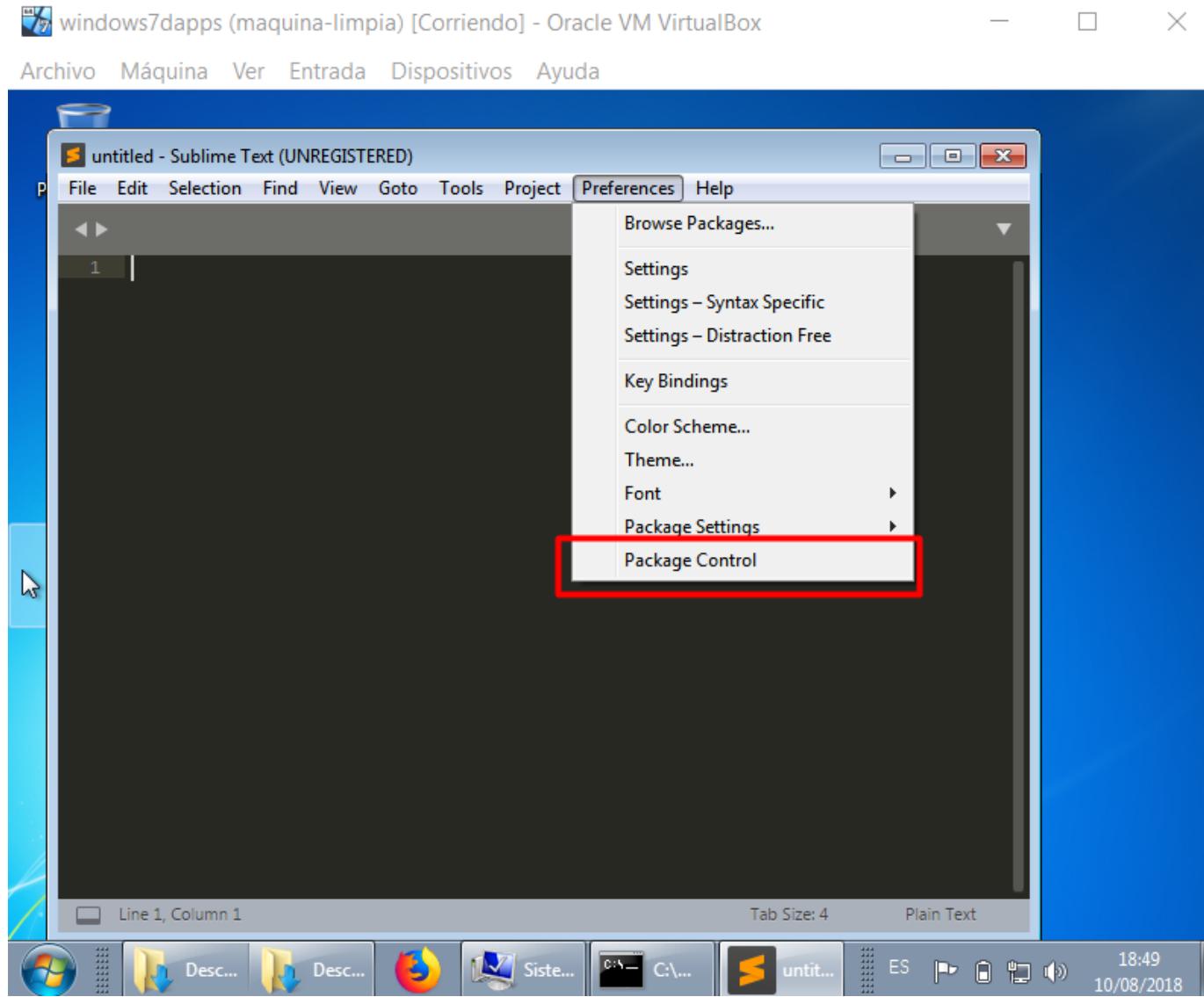
Demo: Install MetaMask



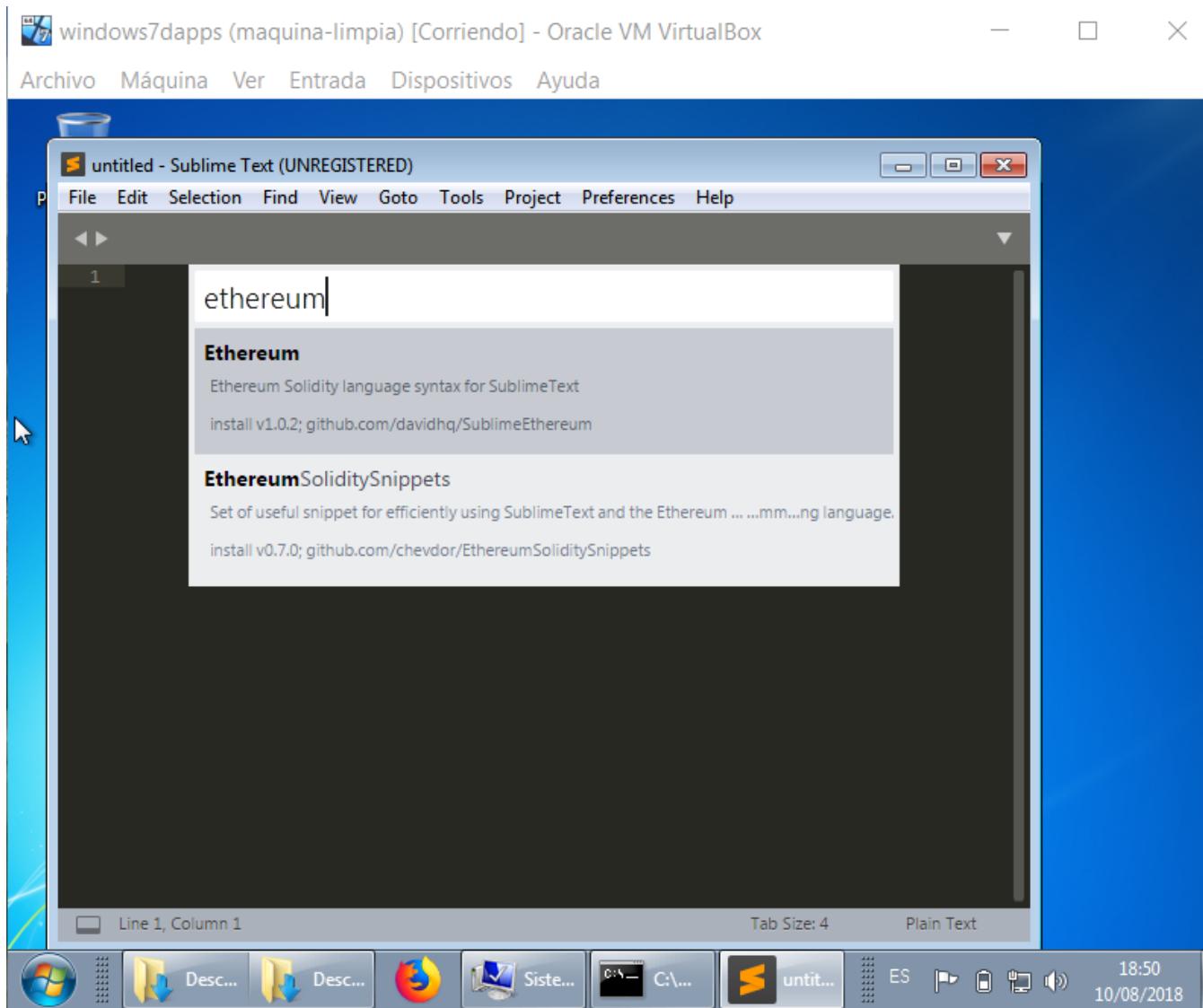
Demo : Install Sublime Text Package



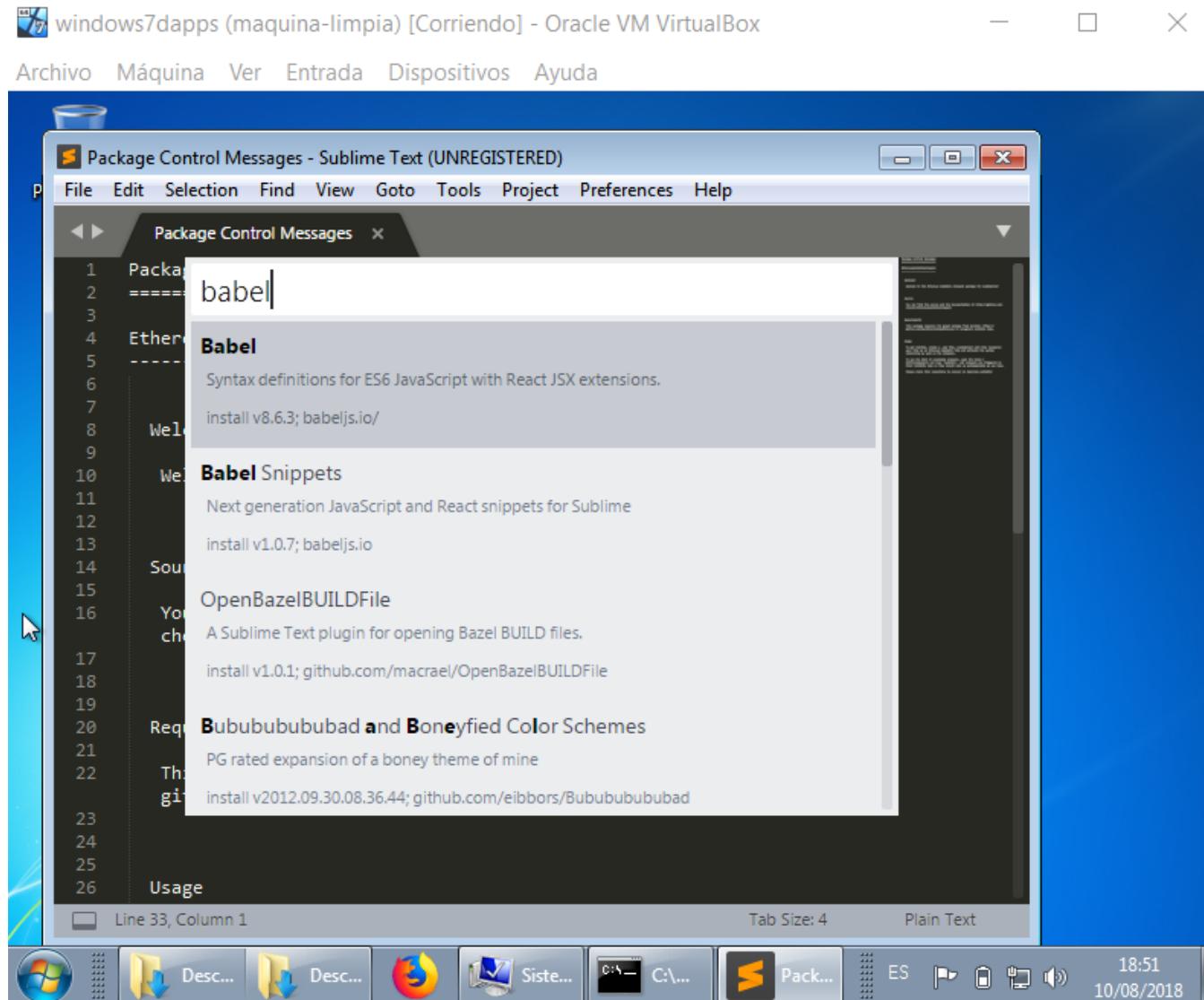
Demo : Install Sublime Text Package



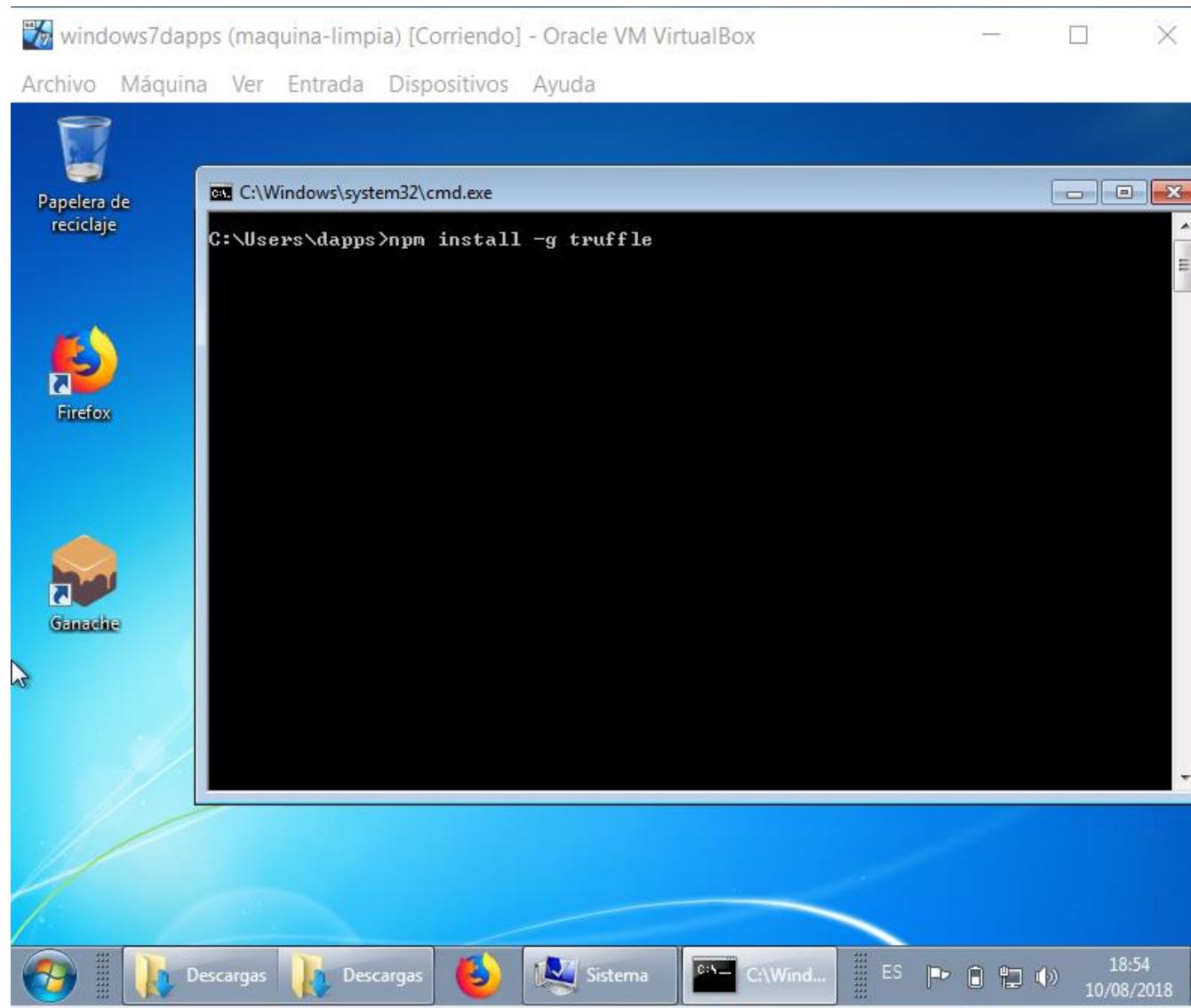
Demo: Install Sublime Text Package



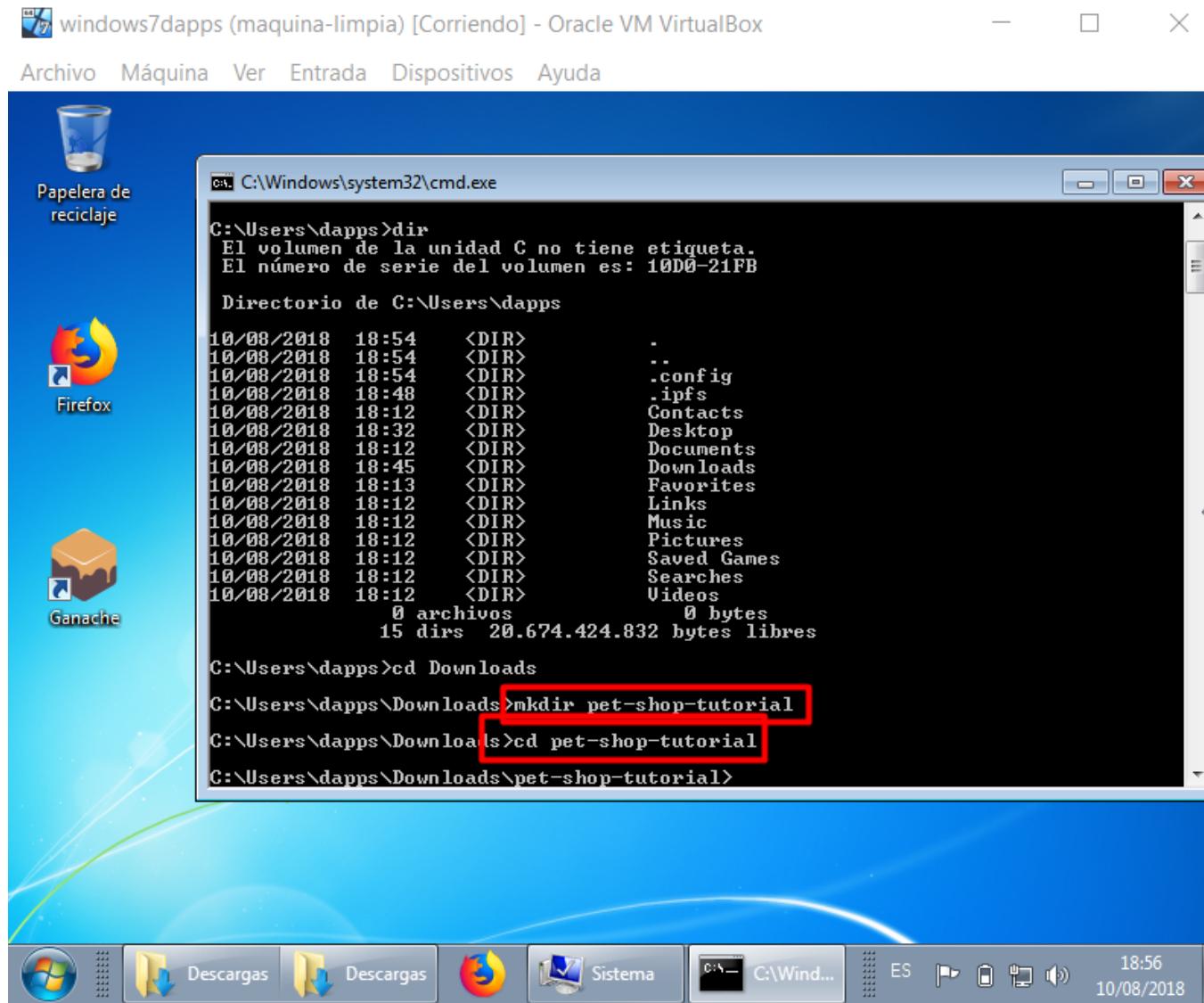
Demo: Install Sublime Text Package



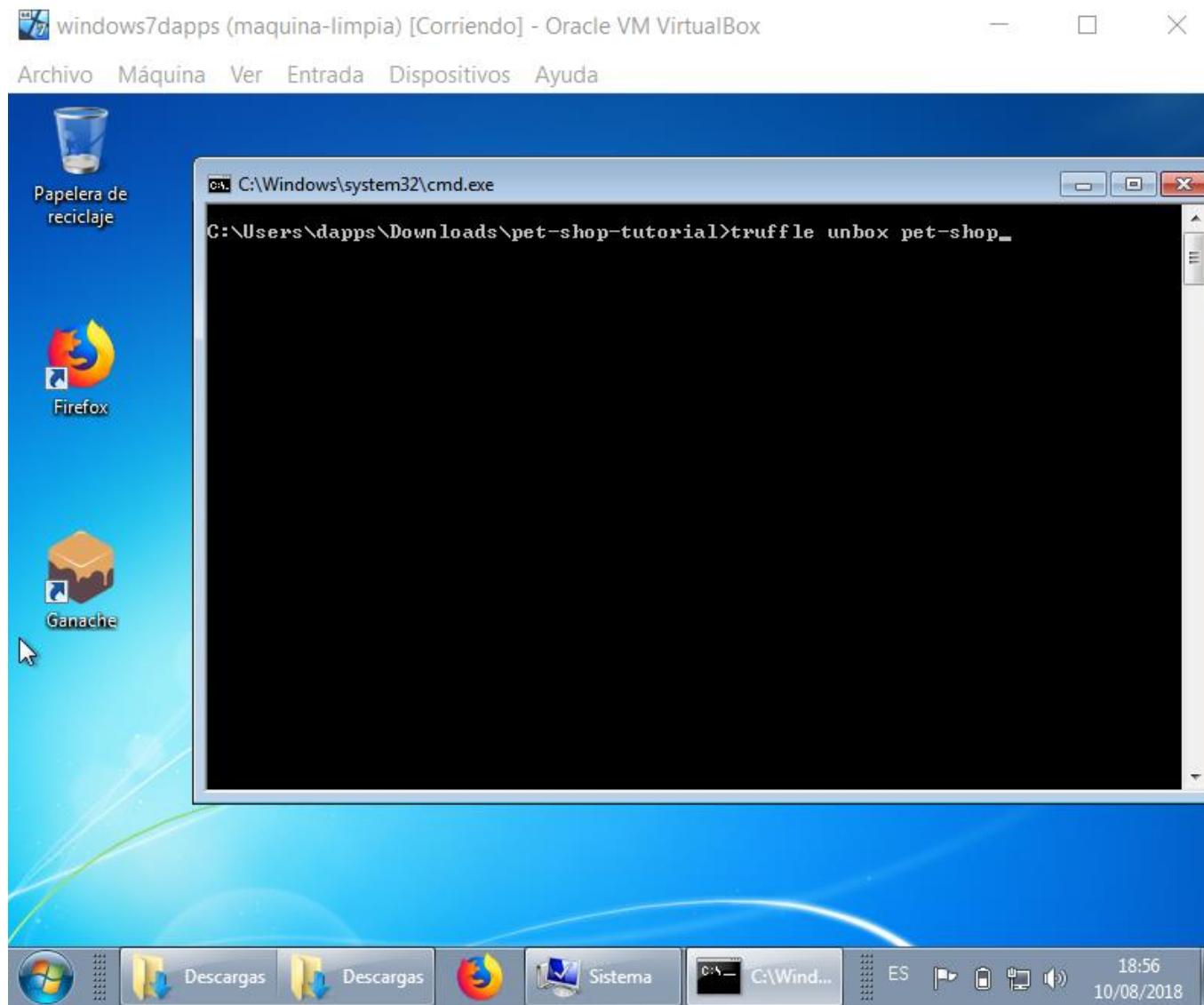
Demo: Install Truffle



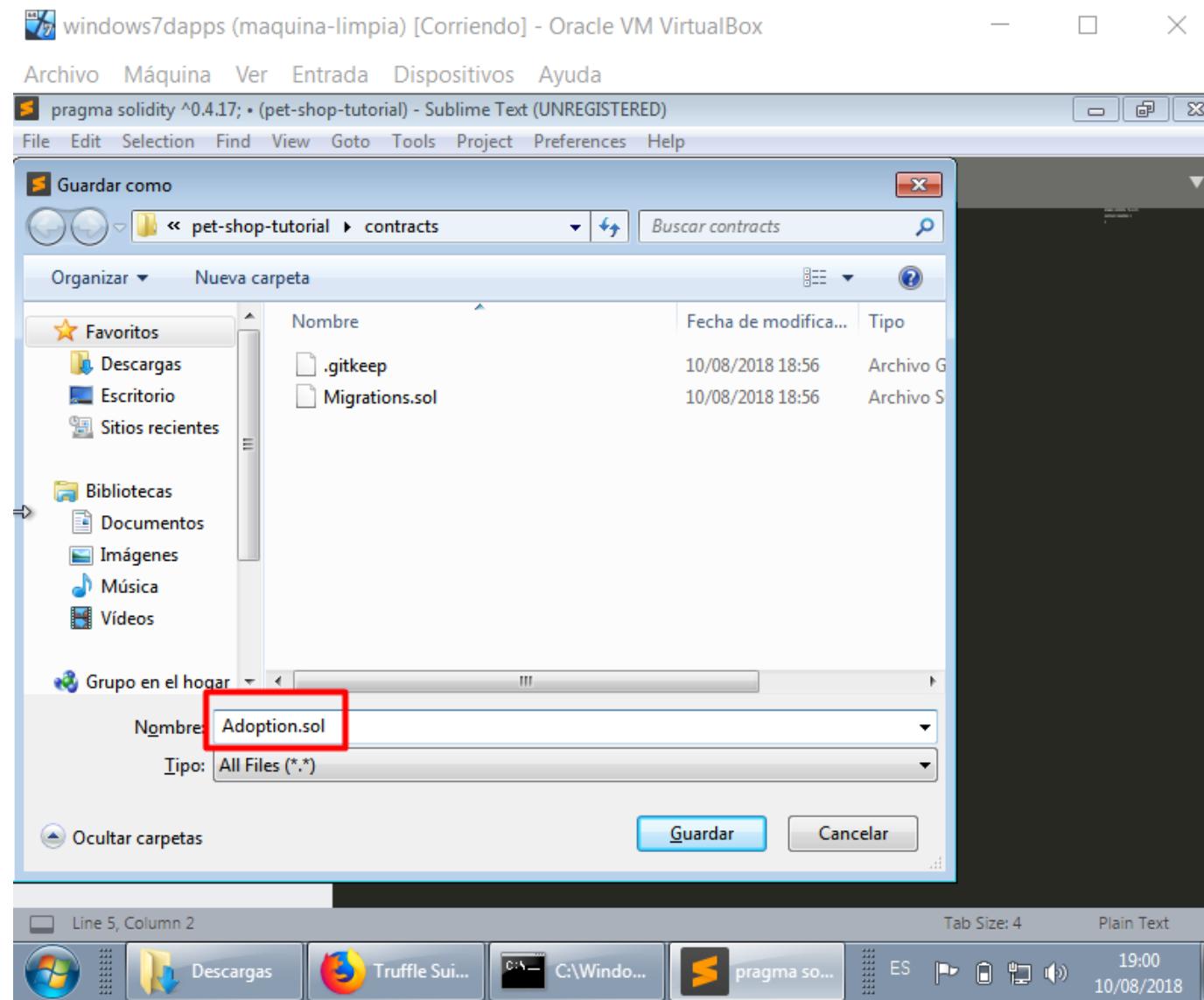
Demo: Install Truffle



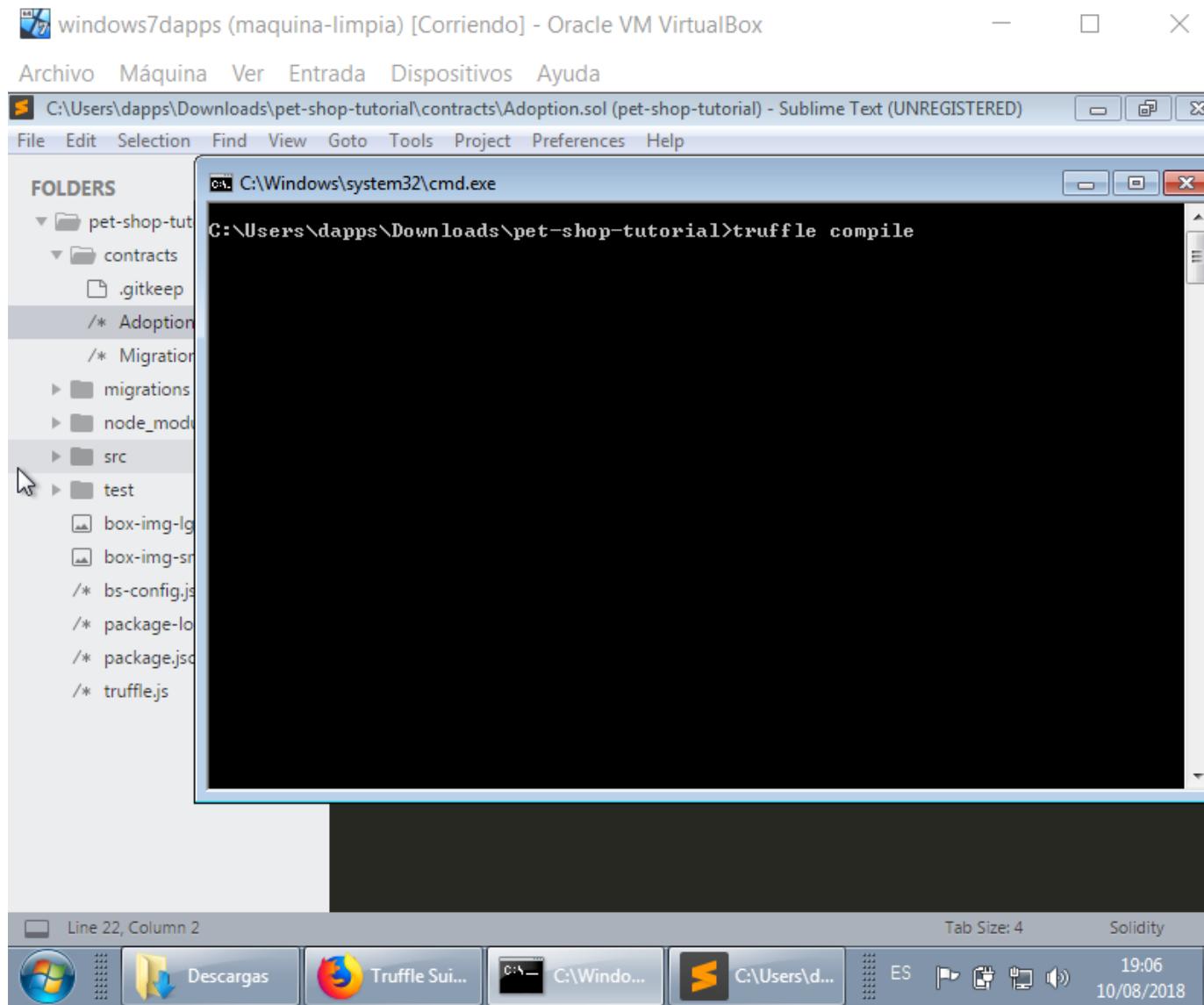
Demo: Install Truffle Box



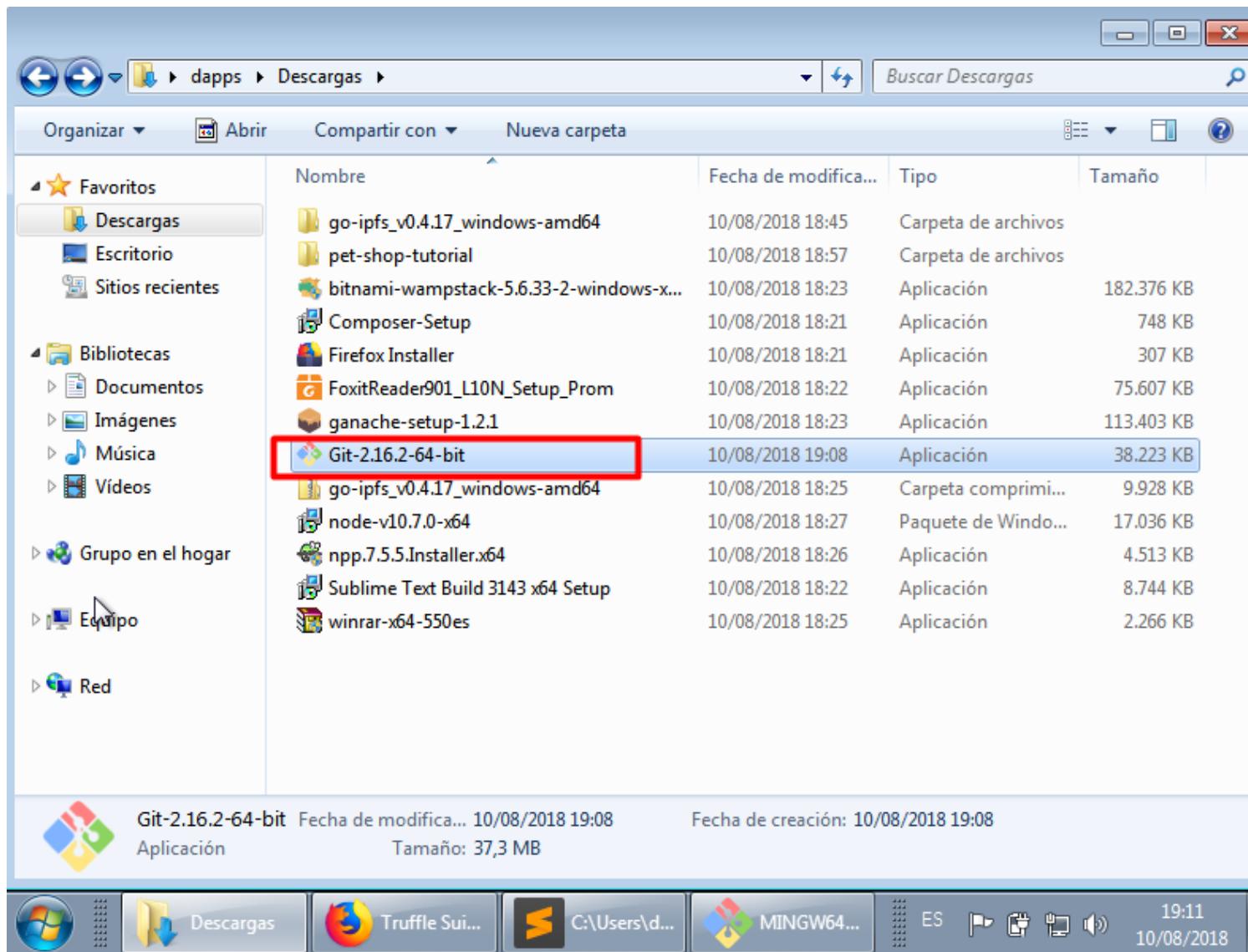
Demo: Create Adoption.sol



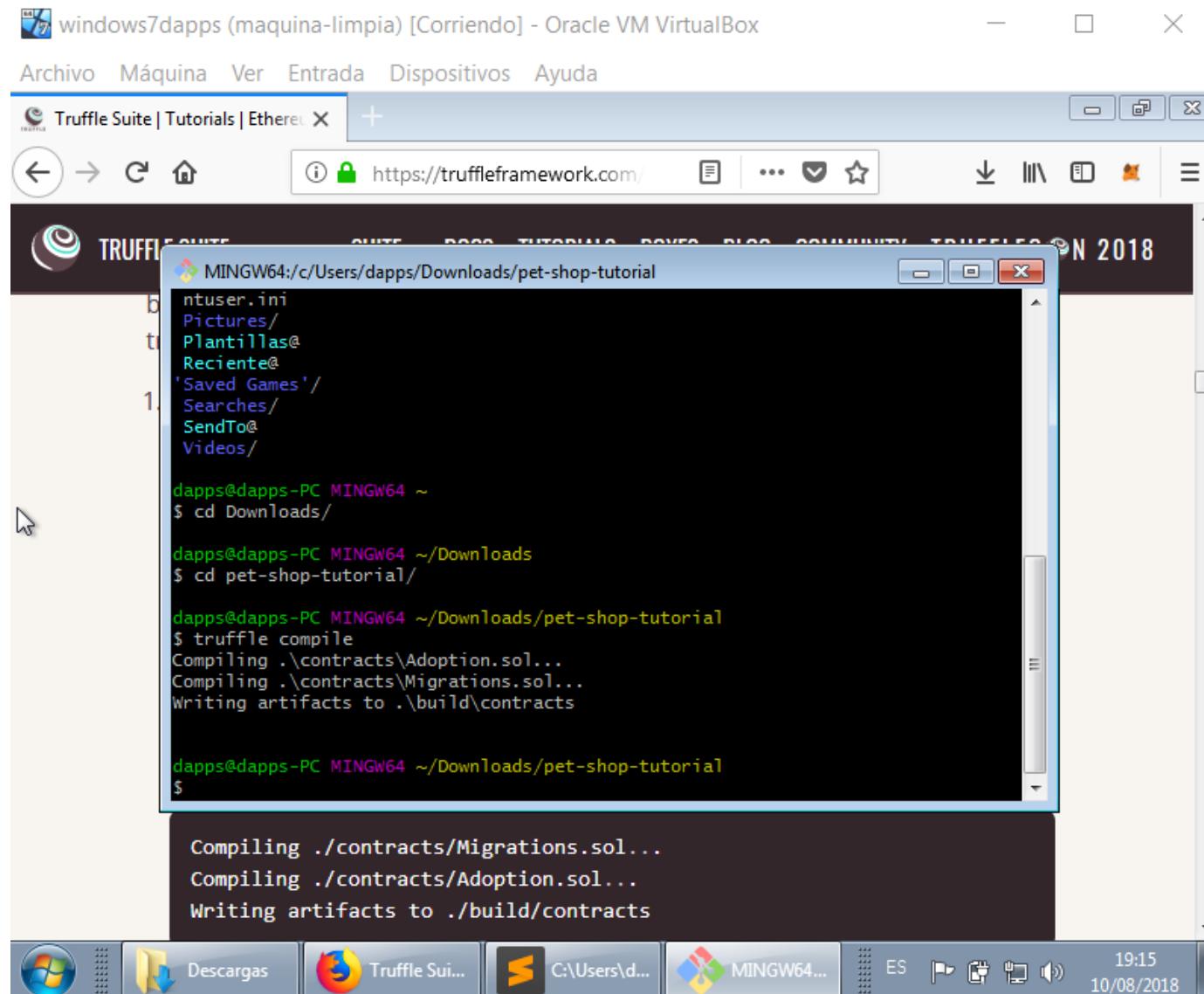
Demo: Truffle Compile



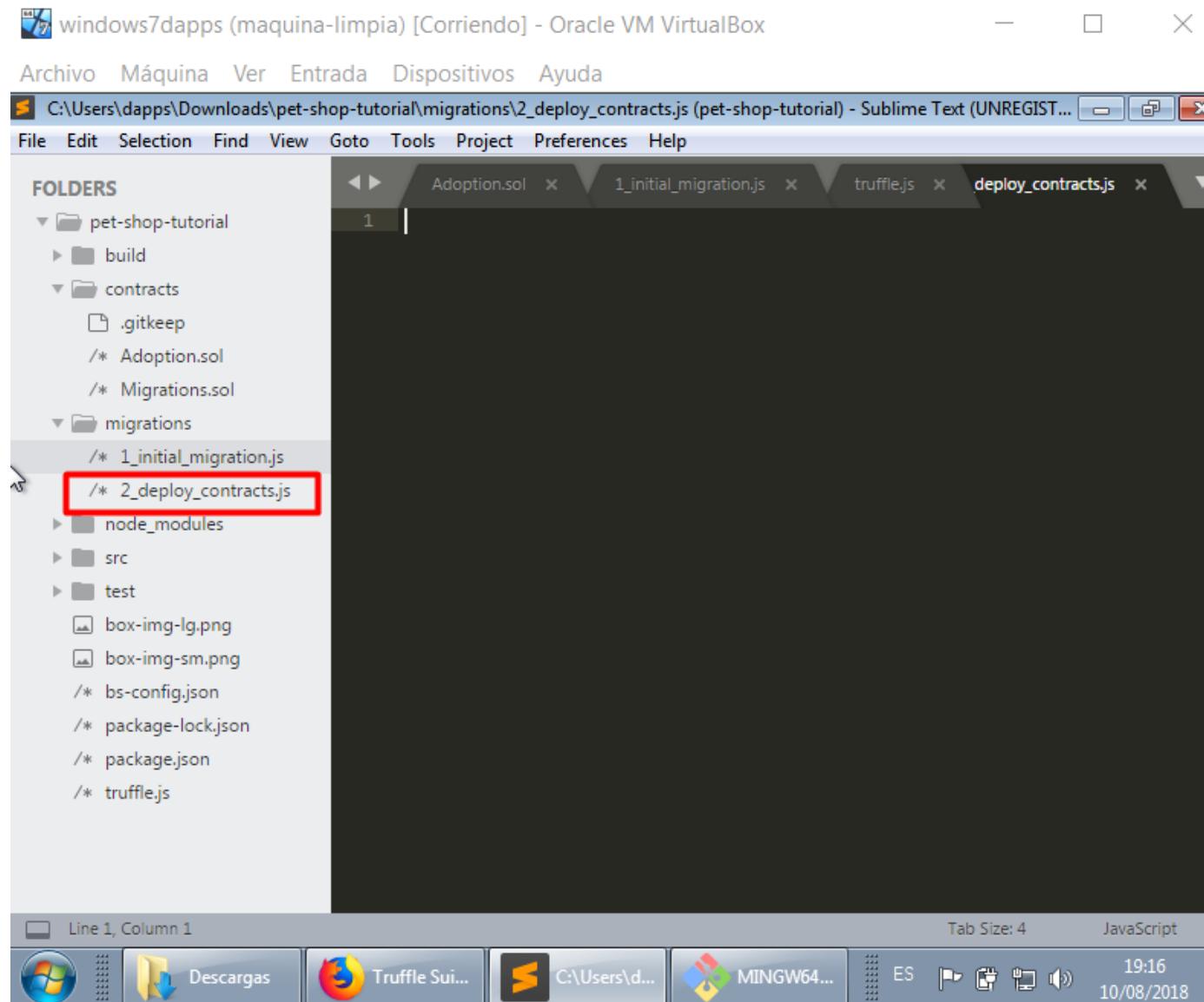
Demo: Install Git Bash



Demo: Truffle Compile



Demo: Create file to migrate Contract

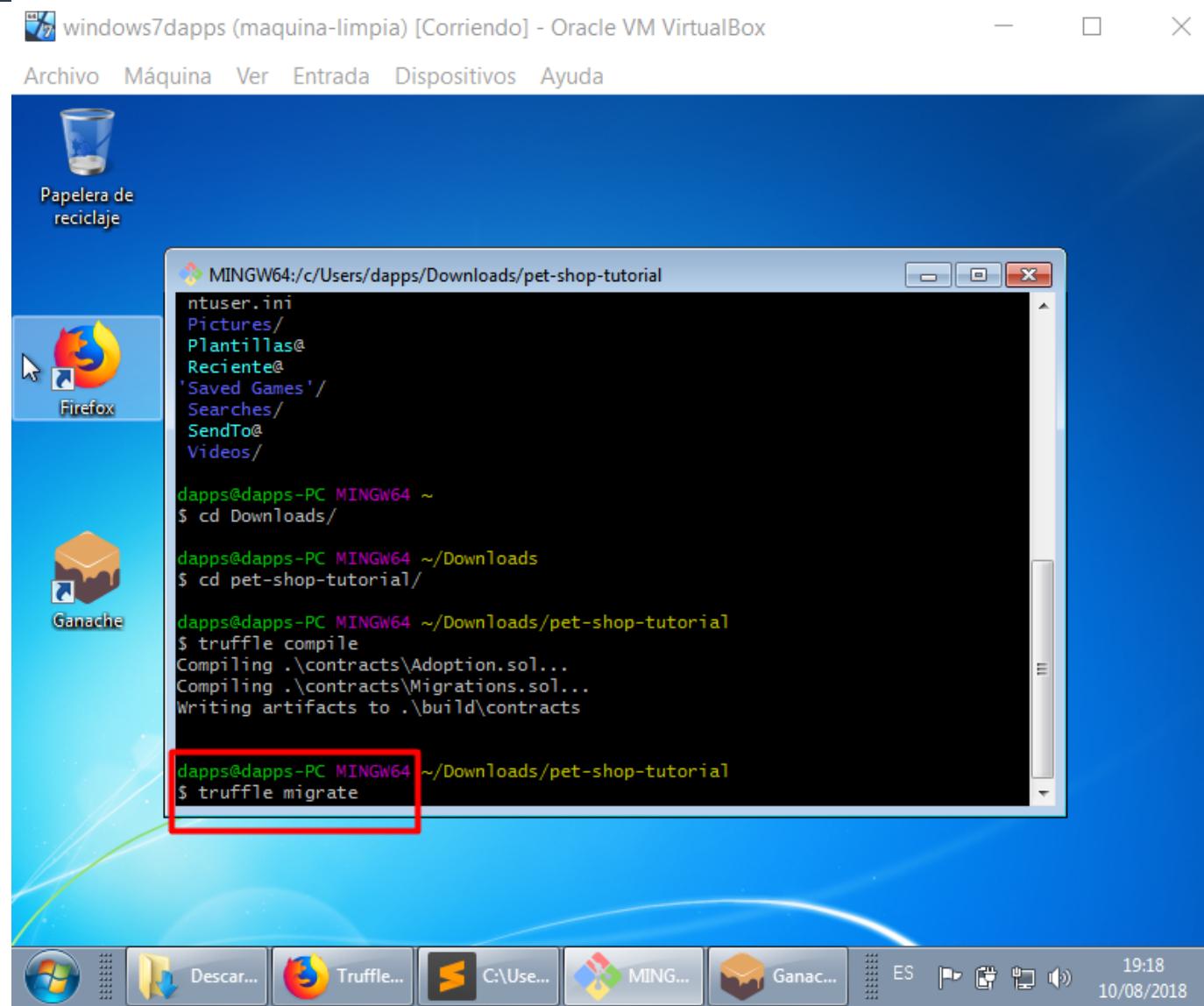


Demo: Ganache Interface

The screenshot shows the Ganache interface running in a VirtualBox window. The top bar includes the title "windows7dapps (maquina-limpia) [Corriendo] - Oracle VM VirtualBox" and standard window controls. The menu bar has options: Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. The main window has a header "Ganache" with tabs: ACCOUNTS (selected), BLOCKS, TRANSACTIONS, LOGS, and a search bar: "SEARCH FOR BLOCK NUMBERS OR TX HASHES". Below the header are status indicators: CURRENT BLOCK 0, GAS PRICE 20000000000, GAS LIMIT 6721975, NETWORK ID 5777, RPC SERVER HTTP://127.0.0.1:7545 (highlighted with a red box), and MINING STATUS AUTOMINING.

ADDRESS	BALANCE	TX COUNT	INDEX	ETH
0xb0507fb38ac544a8da12caf229ccfa68191fe324	100.00	0	0	
0x7399e63b93f9b3736bfaf47b0a853886eac153bf	100.00	0	1	
0x7f56f6aa7a9df766059d172f5f3080707cde0c5d	100.00	0	2	

Demo: Truffle Migrate



Demo: Ganache transactions

The screenshot shows the Ganache application running in a VirtualBox window on a Windows 7 machine. The interface includes a header with 'Ganache' logo, navigation tabs (ACCOUNTS, BLOCKS, TRANSACTIONS, LOGS), and system status (CURRENT BLOCK: 4, GAS PRICE: 20000000000, GAS LIMIT: 6721975, NETWORK ID: 5777, RPC SERVER: HTTP://127.0.0.1:7545, MINING STATUS: AUTOMINING). Below this is a mnemonic seed phrase: mom sunset museum screen pistol burden kite weather key army choose entire. The main content displays four accounts with their addresses and ETH balances:

ADDRESS	BALANCE
0xb0507fb38ac544a8da12caf229ccfa68191fe324	99.94 ETH
0x7399e63b93f9b3736bfaf47b0a853886eac153bf	100.00 ETH
0x7f56f6aa7a9df766059d172f5f3080707cde0c5d	100.00 ETH
0x3c742d300299f8e8d906b47482963b2f5fe99e08	100.00 ETH

The bottom of the screen shows the Windows taskbar with icons for File Explorer, Descargar, Truffle, C:\User..., Ming..., Ganache, and several system icons. The date and time are shown as 19:18 10/08/2018.

Demo: Truffle Front-End

The screenshot shows a Sublime Text window with multiple tabs open: 1_initial_migration.js, truffle.js, 2_deploy_contracts.js, and app.js. The app.js tab is active and contains the following code:

```
    ...
    }
}
}).catch(function(err) {
  console.log(err.message);
});

},
79 handleAdopt: function(event) {
  event.preventDefault();

  var petId = parseInt($(event.target).data('id'));

  /*
  * Replace me...
  */
}

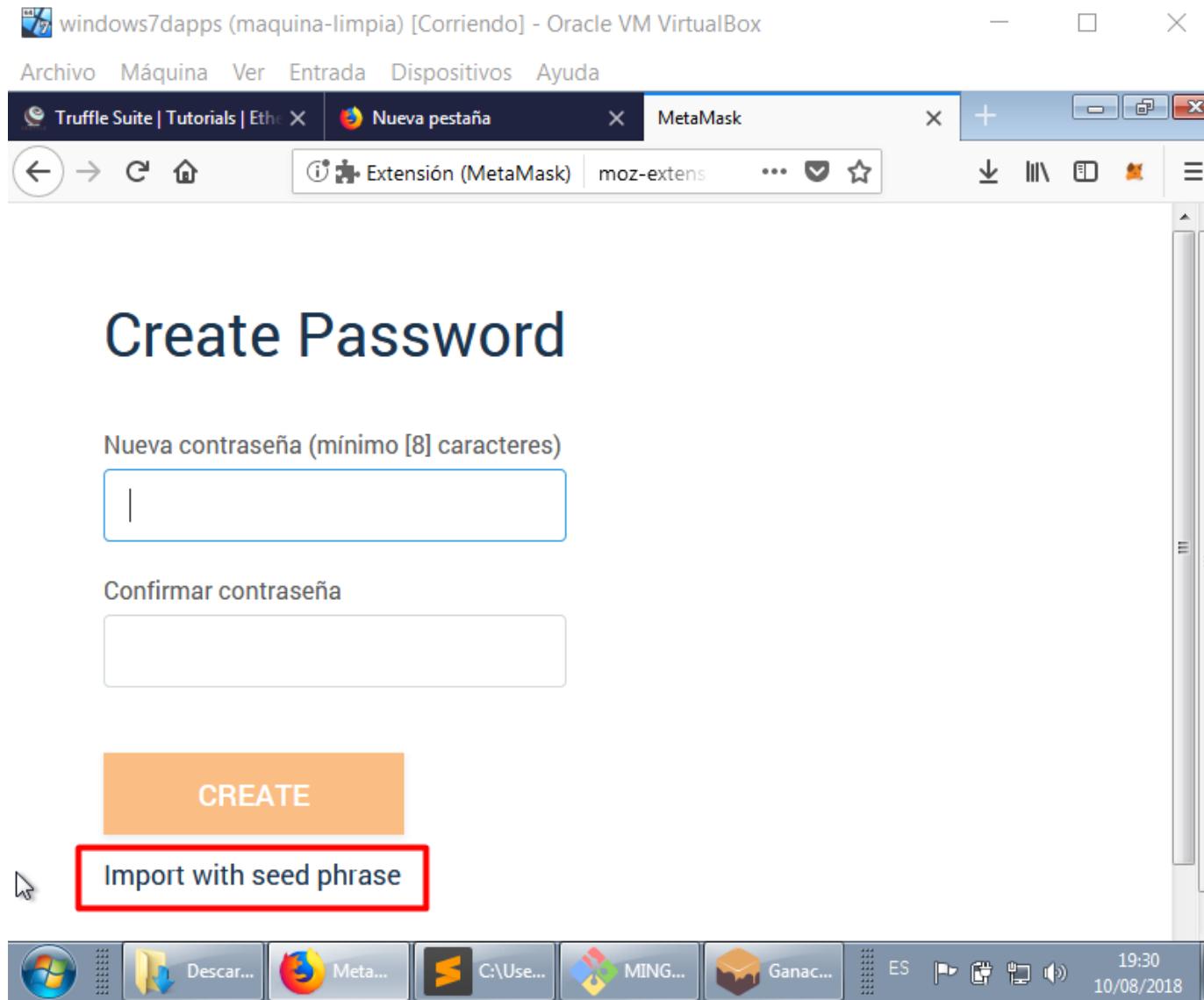
};

$(function() {
  $(window).load(function() {
    App.init();
  });
});
96
```

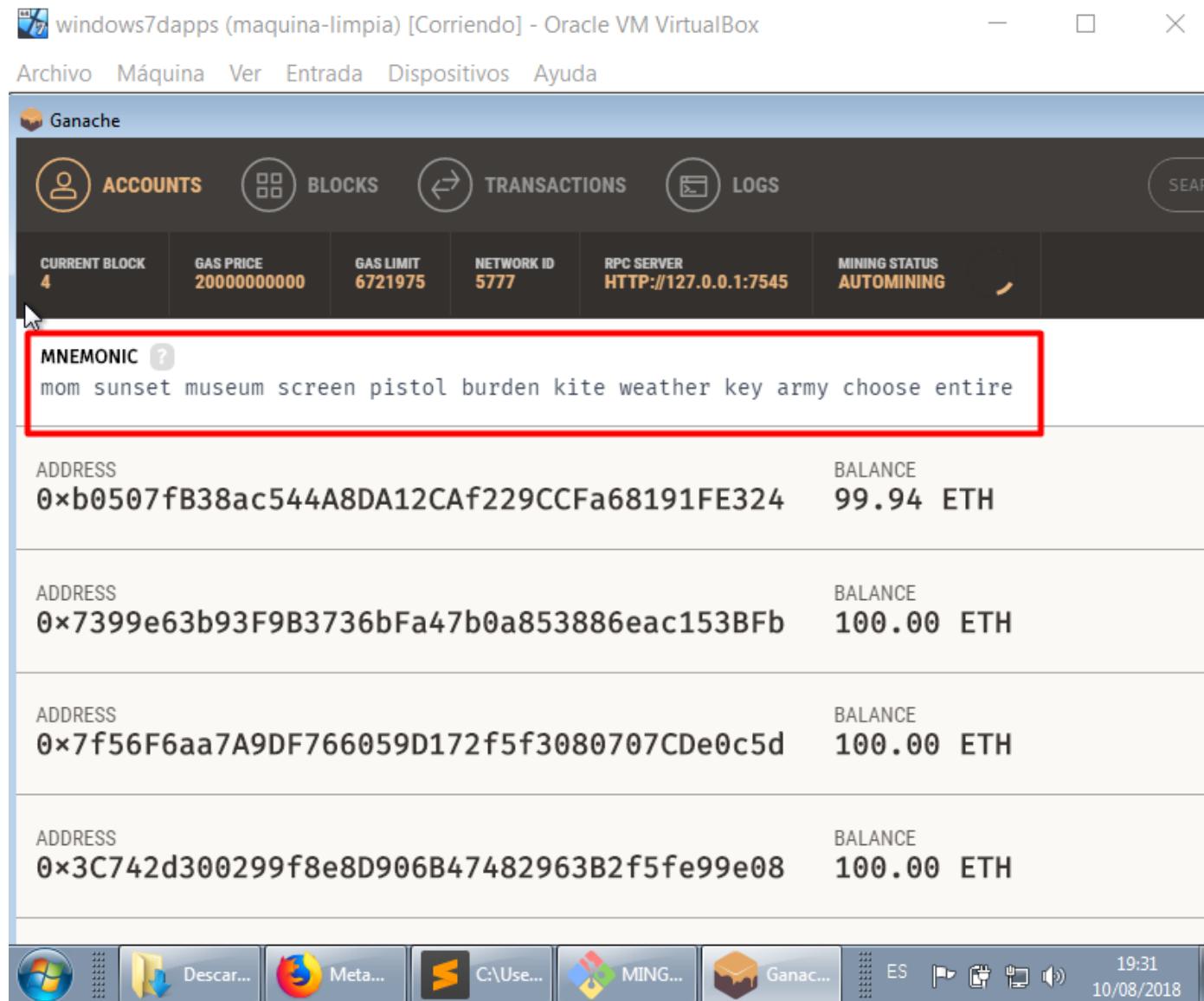
A red box highlights the `handleAdopt` function. The file tree on the left shows the project structure:

- pet-shop-tutorial
 - build
 - contracts
 - .gitkeep
 - /* Adoption.sol
 - /* Migrations.sol
 - migrations
 - /* 1_initial_migration.js
 - /* 2_deploy_contracts.js
 - node_modules
 - src
 - css
 - fonts
 - images
 - js
 - /* app.js
 - /* bootstrap.min.js
 - /* truffle-contract.js
 - /* web3.min.js
- index.html

Demo: Conect MetaMask and Ganache



Demo: Conect Metamask and Ganache



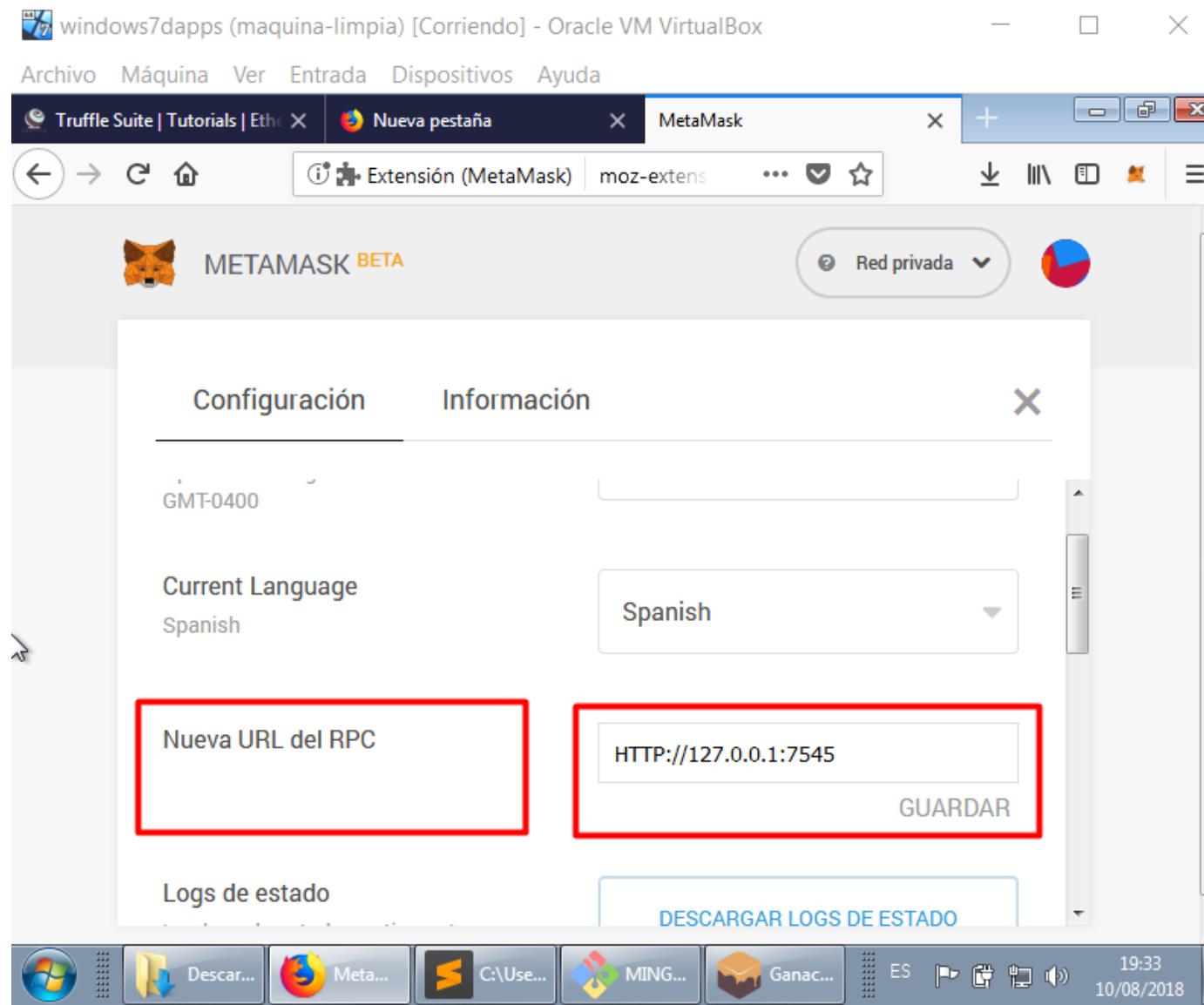
The screenshot shows the Ganache interface running in a VirtualBox window. The top navigation bar includes options like Archivo, Máquina, Ver, Entrada, Dispositivos, and Ayuda. The main header has a Ganache logo and tabs for ACCOUNTS, BLOCKS, TRANSACTIONS, and LOGS. A search bar is on the right. Below the header, network status information is displayed: CURRENT BLOCK 4, GAS PRICE 20000000000, GAS LIMIT 6721975, NETWORK ID 5777, RPC SERVER HTTP://127.0.0.1:7545, and MINING STATUS AUTOMINING.

A red box highlights the MNEMONIC section, which contains the seed phrase: mom sunset museum screen pistol burden kite weather key army choose entire.

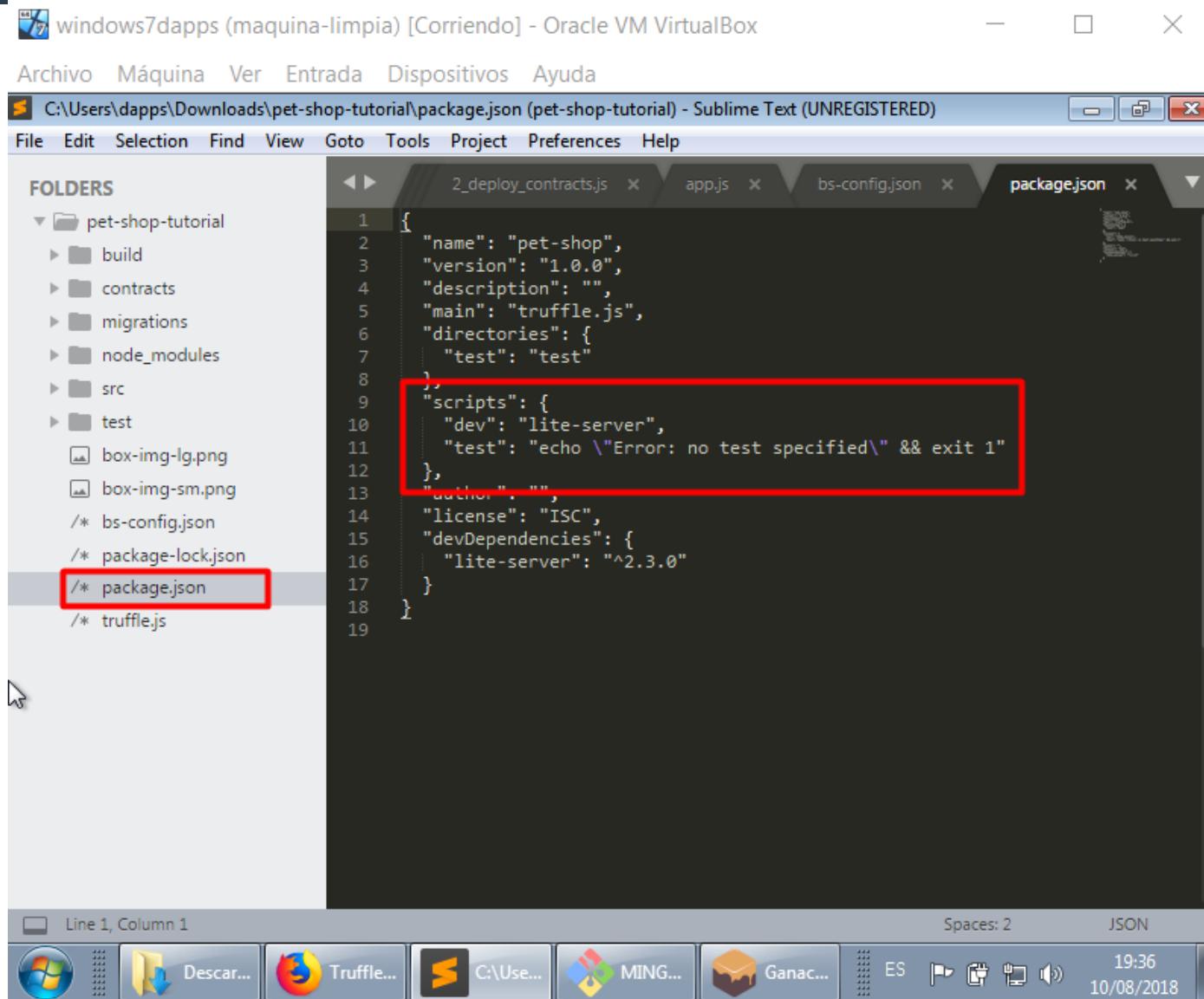
ADDRESS	BALANCE
0xb0507fB38ac544A8DA12CAF229CCFa68191FE324	99.94 ETH
0x7399e63b93F9B3736bFa47b0a853886eac153BFb	100.00 ETH
0x7f56F6aa7A9DF766059D172f5f3080707CDe0c5d	100.00 ETH
0x3C742d300299f8e8D906B47482963B2f5fe99e08	100.00 ETH

The taskbar at the bottom shows icons for Windows, Downloads, Mozilla Firefox, C:\Use..., Ming... (with a yellow diamond icon), Ganac... (with a brown cake icon), and several system icons. The date and time are shown as 19:31 10/08/2018.

Demo: Conect Metamask and Ganache



Demo: Config server for Front-End

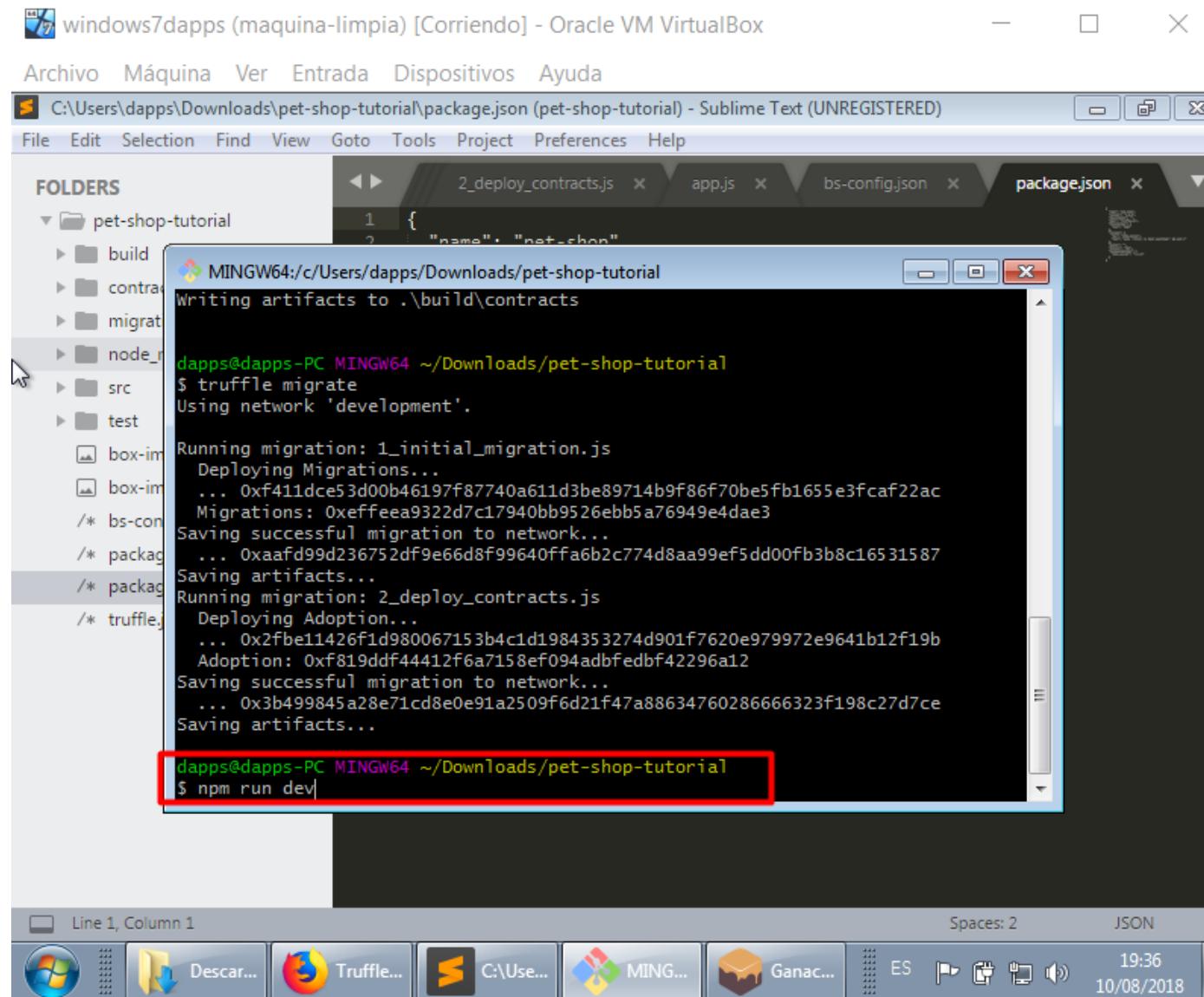


The screenshot shows a Sublime Text window with multiple tabs open. The current tab is `package.json`, which contains the following JSON code:

```
1 {  
2   "name": "pet-shop",  
3   "version": "1.0.0",  
4   "description": "",  
5   "main": "truffle.js",  
6   "directories": {  
7     "test": "test"  
8   },  
9   "scripts": {  
10    "dev": "lite-server",  
11    "test": "echo \\\"Error: no test specified\\\" & exit 1"  
12  },  
13  "author": "",  
14  "license": "ISC",  
15  "devDependencies": {  
16    "lite-server": "^2.3.0"  
17  }  
18}  
19
```

A red box highlights the `scripts` section of the JSON object. The sidebar on the left shows the project structure under the `pet-shop-tutorial` folder, including `build`, `contracts`, `migrations`, `node_modules`, `src`, `test`, and files like `box-img-lg.png` and `bs-config.json`. A file named `/* package.json` is also listed in the sidebar.

Demo: Start Server for Front-End



Demo: Use our Dapp

windows7dapps (maquina-limpia) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Truffle Suite | Tuto X Nueva pestaña X MetaMask X Pete's Pet Shop X

localhost:3000

Breed: Scottish Terrier
Age: 3
Location: Lisco, Alabama

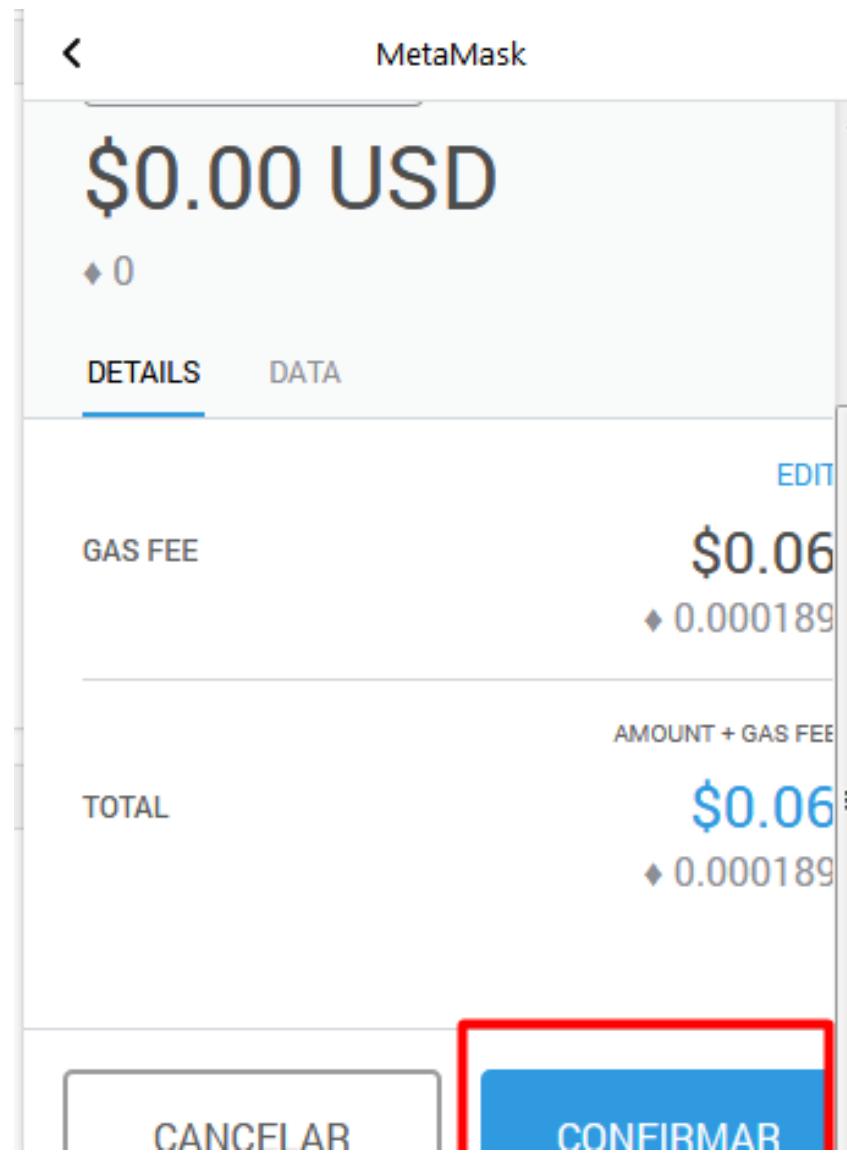
Breed: Scottish Terrier
Age: 3
Location: Tooleville, West Virginia

Collins

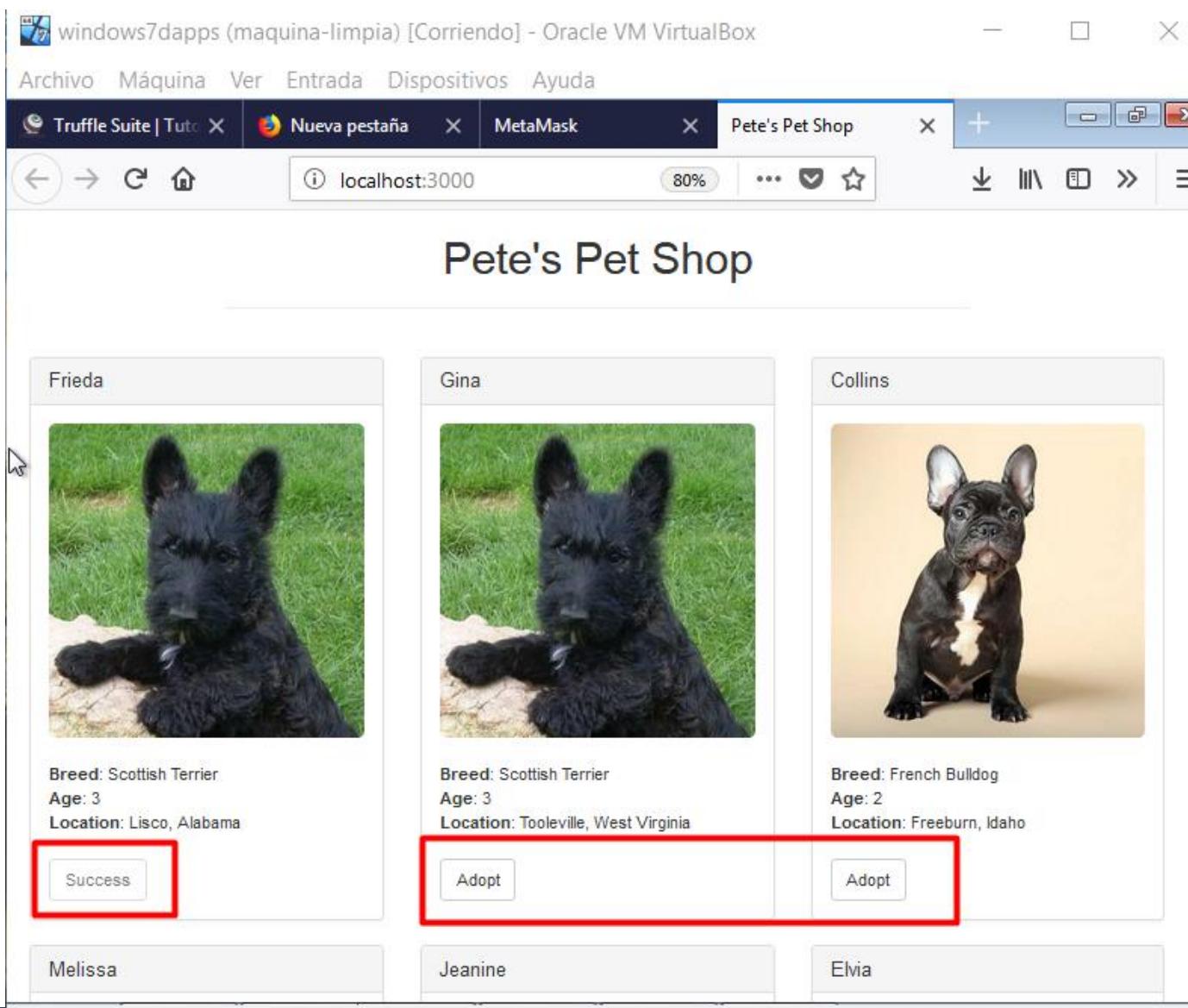
Melissa

ES Descar... Pete's ... C:\Use... MING... Ganac... 19:37 10/08/2018

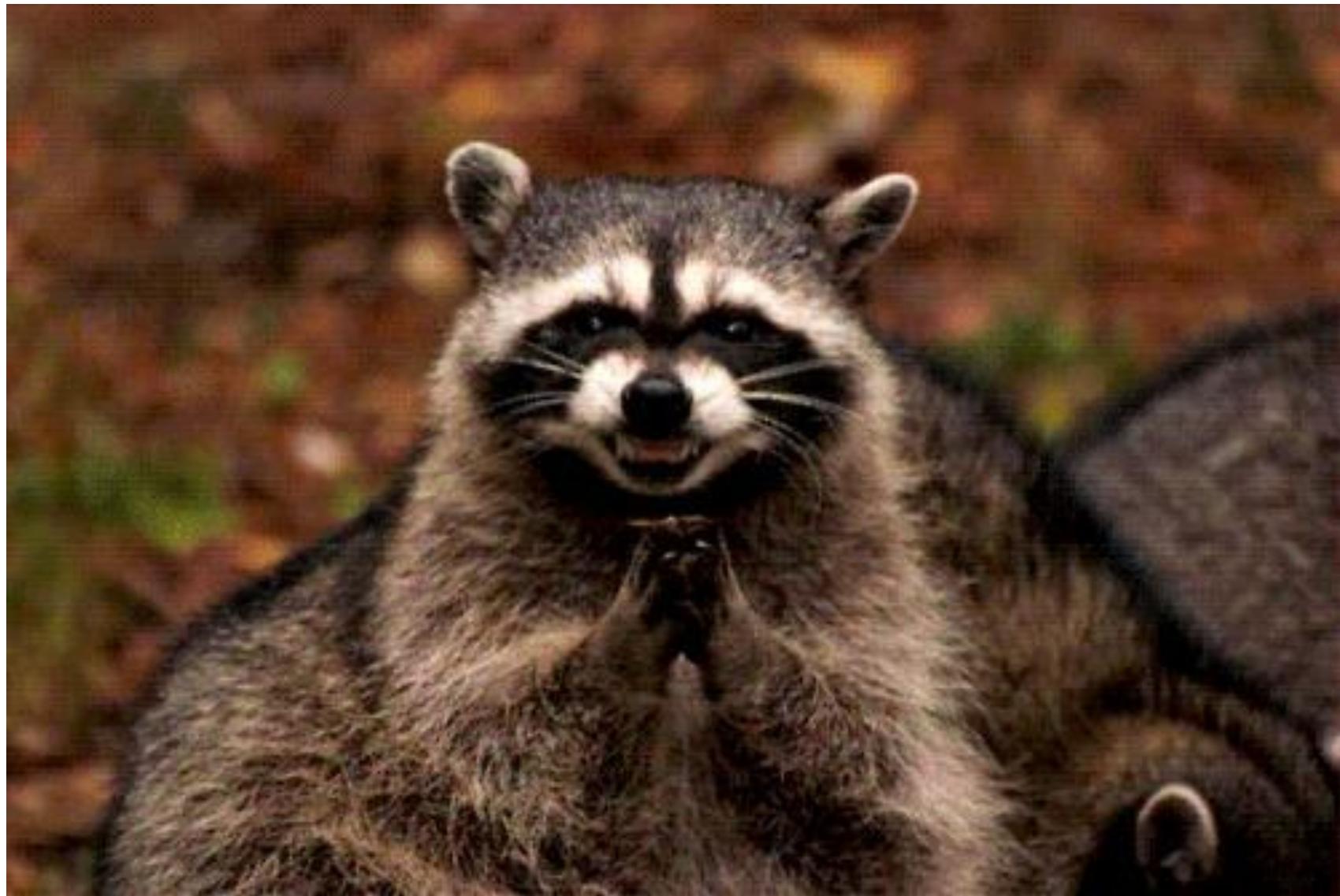
Demo: Use our Dapp



Demo: Use our Dapp



Bads things for Blockchain Developers



Bads things for Blockchain Developers

≡ BUSINESS INSIDER
ESPAÑA

TECNOLOGÍA

TECNOLOGÍA

Pierden medio millón en criptomonedas y acusan al informático: "El error es de la empresa"

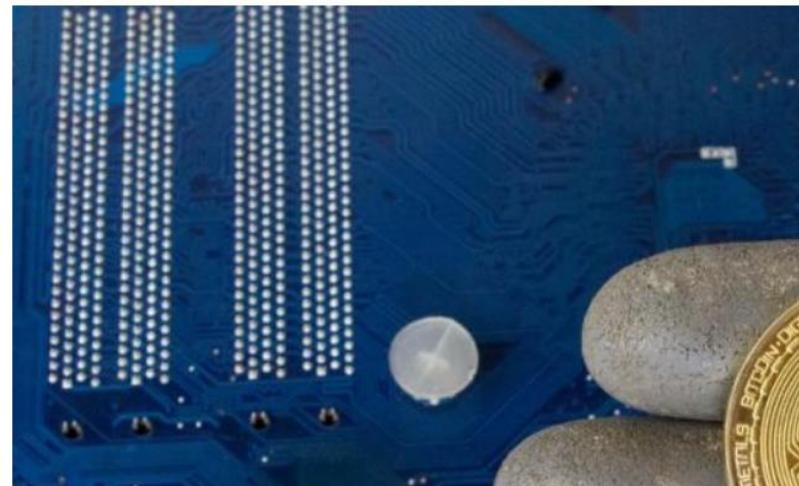
Analía Plaza ⌚ 1 Abr 2018 21:01h.

 FACEBOOK

 TWITTER

 LINKEDIN

 FLIPBOARD



Bads things for Blockchain Developers

El fallo estuvo en unas comillas: al desplegar el código (al ponerlo en marcha), olvidaron entrecomillar la dirección de Ethereum (una serie de letras y números) donde debían recibir el dinero y JavaScript, el lenguaje de programación usado, lo interpretó de otra manera. Resultado: **todo el dinero ha ido a una cuenta que no es y a la que nadie puede acceder.**

En lugar de escribir esto: `web3.toHex("0x132623d797FE61f8E1D1aE2aA17Fc997a4f9bf77")`
Escribieron esto, sin
comillas: `web3.toHex(0x132623d797FE61f8E1D1aE2aA17Fc997a4f9bf77)`

Así que en lugar de ir a esta cuenta han ido a esta. En blockchain, cada clave pública lleva asociada una clave privada: en este caso, nadie tiene la clave privada asociada a la clave pública en la que está el dinero perdido.



Bads things for Blockchain Developers

Etherscan
The Ethereum Block Explorer

Address 0x132623d797FE61f8E1D1aE2aA17Fc997a4f9bf77

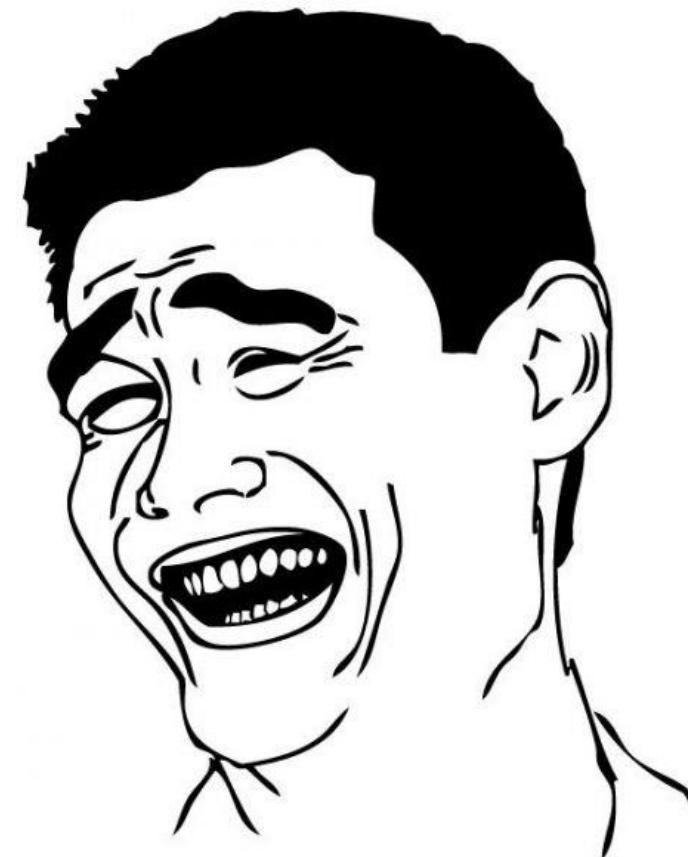
Sponsored: Color - Revolutionizing the Dapp Ecosystem, Bounty & Airdrop, Get 240,000 COL NOW!

Overview

Balance:	0.319141366 Ether
Ether Value:	\$91.72 (@ \$287.41/ETH)
Transactions:	190 txns

Misc

Address Watch:
Token Balances:



Etherscan
The Ethereum Block Explorer

Address 0x132623d797FE61De05De0aB5ec5E7A8380000000

Sponsored: Color - Revolutionizing the Dapp Ecosystem, Bounty & Airdrop, Get 240,000 COL NOW!

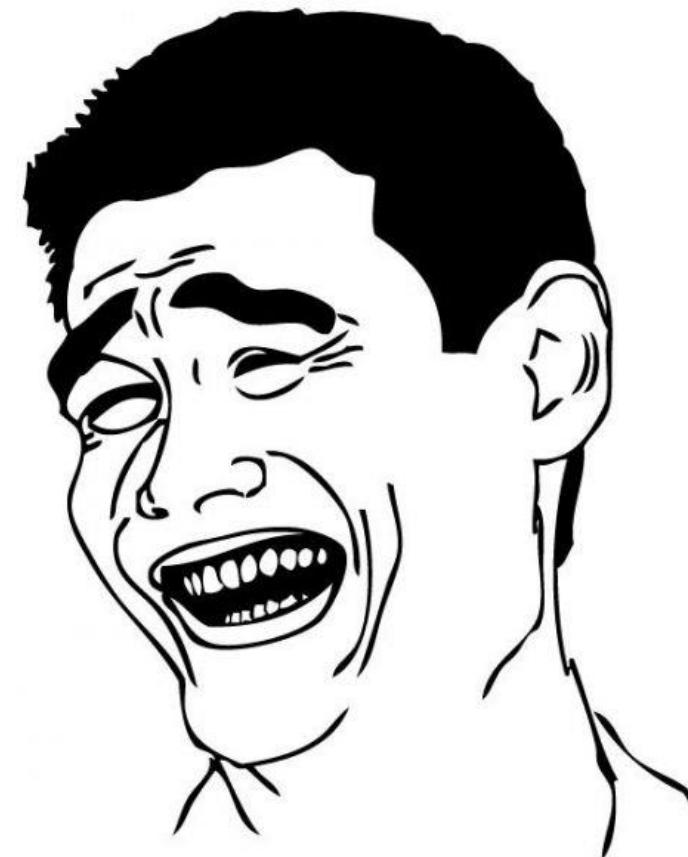
Overview

Balance:	1,006.564437256 Ether
Ether Value:	\$289,296.68 (@ \$287.41/ETH)
Transactions:	0 txns

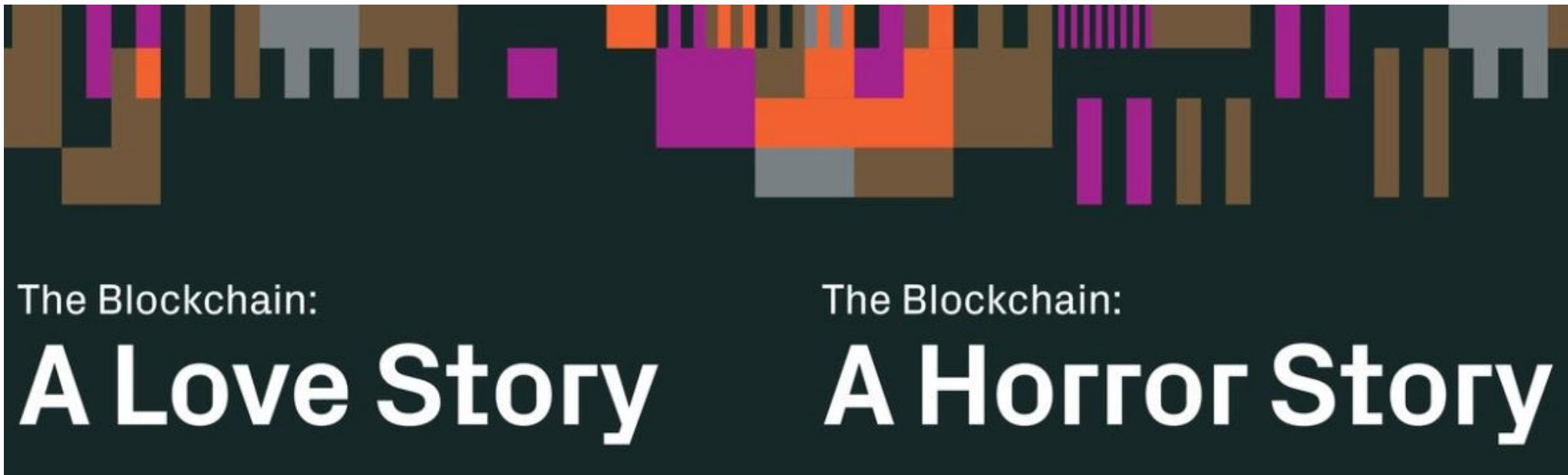
Misc

Address Watch:
Token Balances:

View (\$0.00) ▾



Bads things for Blockchain Developers



BUSINESS 06.19.18 06:00 AM

The Blockchain:
A Love Story

The Blockchain:
A Horror Story

INSIDE THE CRYPTO WORLD'S
BIGGEST SCANDAL

BY JEFFREY WALTERS | PHOTOS BY ANDREW HETHERINGTON FOR BLOOMBERG



Bads things for Blockchain Developers

It was by far the biggest ICO to date, and Gevers was ecstatic. “TEZOS RAISES RECORD-BREAKING \$200 MILLION IN THREE DAYS,” he tweeted, “giving it the resources to grow into one of the Big 3 blockchains.”



Bads things for Blockchain Developers



Bads things for Blockchain Developers

The screenshot shows a Reddit post on the r/ethereum subreddit. The post is titled "Current Ethereum blockchain size?" and has 15 upvotes. The poster asked for projections for the end of 2017. The post has 10 comments, was shared, saved, and upvoted 84%. A note indicates the thread is archived. The post is sorted by top suggestions.

Posted by u/holabebe 1 year ago

15 Current Ethereum blockchain size?

And projections for the end of 2017??

10 Comments Share Save ... 84% Upvoted

This thread is archived
New comments cannot be posted and votes cannot be cast

SORT BY TOP (SUGGESTED)

3esmit 6 points · 1 year ago

Blockchain size in ethereum depends in the implementation. In Parity is about 6 GB, in Geth is about 11 GB. Geth is not implementing state pruning, so 11 GB would be a clean sync with --light, while if you don't use this would be 60GB+. See this <http://ethereum.stackexchange.com/questions/143/what-are-the-ethereum-disk-space-needs> You might also want to know the size of the 'exported' blockchain, which I don't know.

Share Save

mcgravier 6 points · 1 year ago

clean sync with --light

You mean --fast. Light is experimental and doesn't require blockchain download at all

Share Save

3esmit 2 points · 1 year ago

Ops! Thanks for the correction, yes, --fast, not --light.

Share Save

Bads things for Blockchain Developers

Esta solución halla su razón de ser en que, actualmente, los dos principales *blockchains*, *Bitcoin* y *Ethereum*, todavía son bastante limitados en cuanto a la cantidad de transacciones que pueden procesarse en un momento dado. Esto da como resultado casos en los que una sola transacción puede poner a la red en una situación de conmoción.

Un ejemplo común de cómo estos problemas de escalabilidad están limitando la competitividad de *Blockchain* con los sistemas centralizados es la comparación con VISA. Mientras que el popular proveedor de tarjetas de crédito maneja hasta 2.000 transacciones por segundo, *Ethereum* tiene actualmente un límite de aproximadamente 15 transacciones por segundo.

Goods things for Blockchain Developers



Goods things for Blockchain Developers

The screenshot shows the homepage of cryptozombies.io. At the top, there's a banner for the **KICKSTARTER** campaign for **Zombie: Battleground**, which is currently in progress. The banner features the **LOOM NETWORK** logo. Below the banner, the main headline reads: **Learn to Code Ethereum DApps By Building Your Own Game**. A subtext explains: **CryptoZombies is an interactive code school that teaches you to write smart contracts in Solidity through building your own crypto-collectables game.** There are two prominent buttons: **Get Started, It's Free** and **Learn More**. A blue ribbon at the bottom has the text **CRYPTOZOMBIES** on it. The background of the page features a dark, atmospheric illustration of a zombie in a graveyard.

Good things for Blockchain Developers



openzeppelin

Smart contracts deployed to the Ethereum mainnet can deal with real money, so having our Solidity code free from errors and highly secure is essential.

[Zeppelin Solutions](#), a smart contract auditing service, has recognized this need. Using their experience, they've put together a set of vetted smart contracts called [OpenZeppelin](#).

We can use and extend these contracts to create more secure dapps in less time. OpenZeppelin comes with a wide array of smart contracts for various important functions ([see them all here](#)), but today we'll be focusing on their token contracts. Specifically, we'll be extending their `StandardToken.sol` contract to create our own [ERC20](#)-compliant token.

Good things for Blockchain Developers

The screenshot shows the Securify website, a security scanner for Ethereum smart contracts. The top navigation bar includes links for Home, About, Products, Services, News, Contact, and Help. The main header features the Securify logo and the tagline "SECURITY SCANNER FOR ETHEREUM SMART CONTRACTS". Below the header, there are two large statistics: "18288 Contracts scanned" with a code icon and "375079 Issues found" with a warning icon. A "STAY UPDATED" button is located at the bottom of this section. To the right, there are two bullet points: "Created by ICE center, ETH Zurich and ChainSecurity AG, a top provider for smart contract audits." and "Based on the latest research, see our technical paper." Social media sharing icons for Twitter, LinkedIn, Facebook, and others are also present. The main content area contains a "SCAN NOW" button, an "info" icon, and three input methods: "PASTE CODE", "UPLOAD ZIP", and "CLONE GIT". Below these is a code editor window showing a snippet of Solidity code:

```
18 contract Ownable {
19     using SafeMath for uint256;
20
21     address owner;
22
23     modifier onlyOwner() {
24         require(msg.sender == owner);
25         _;
26     }
27
28     function transferOwnership(address _owner) {
29         owner = _owner;
30     }
31 }
```

A callout box highlights the line "Contract fields that can be modified by any user must be inspected." with the "info" icon.

Good things for Blockchain Developers

The screenshot shows the Ethereum Remix IDE interface. The left panel displays the Solidity code for a 'Ballot' contract. The right panel contains various development tools and logs.

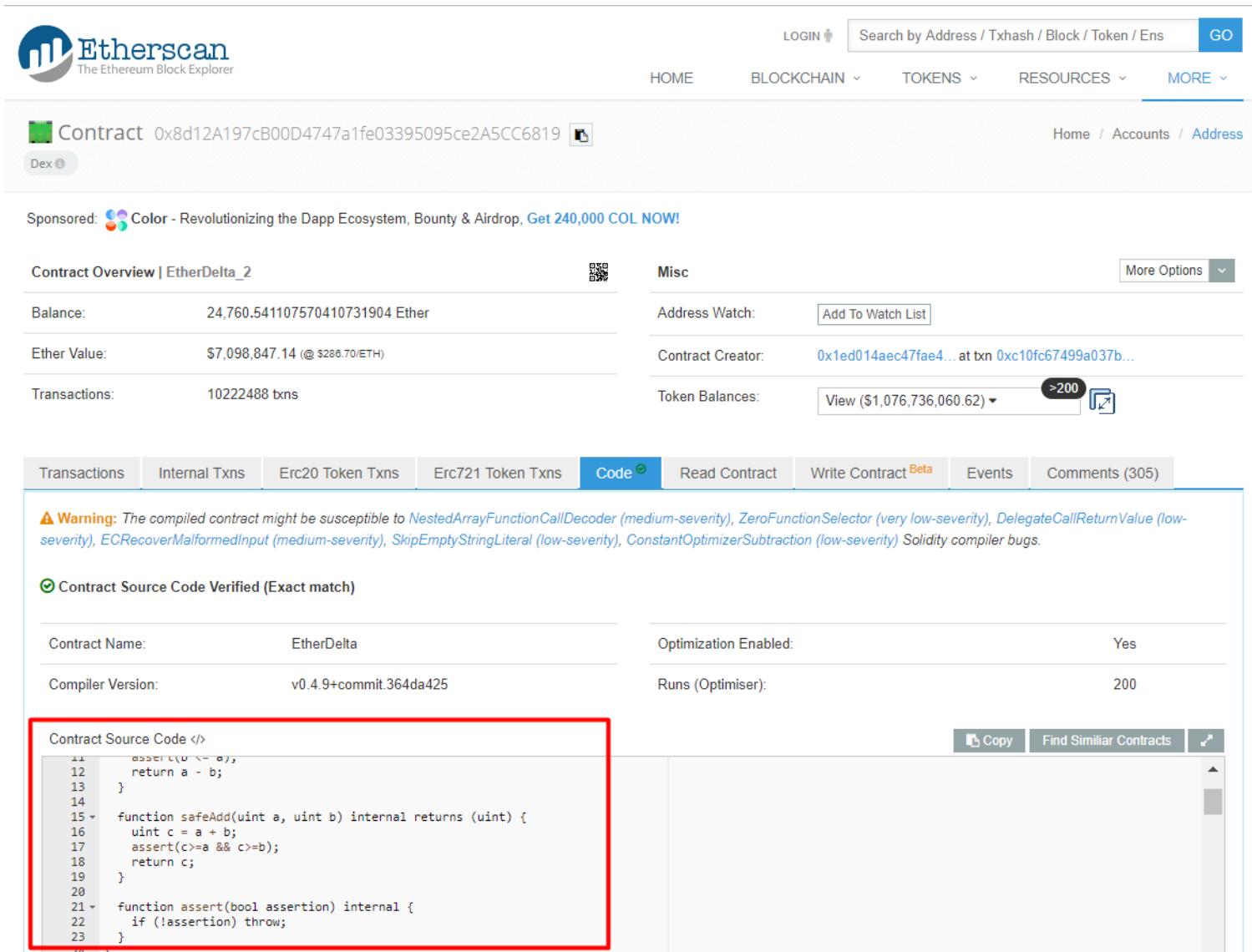
Solidity Contract Code:

```
1 pragma solidity ^0.4.0;
2 contract Ballot {
3
4     struct Voter {
5         uint weight;
6         bool voted;
7         uint8 vote;
8         address delegate;
9     }
10    struct Proposal {
11        uint voteCount;
12    }
13
14    address chairperson;
15    mapping(address => Voter) voters;
16    Proposal[] proposals;
17
18    // Create a new ballot with $_numProposals different proposals.
19    function Ballot(uint8 _numProposals) public {
20        chairperson = msg.sender;
21        voters[chairperson].weight = 1;
22        proposals.length = _numProposals;
23    }
24
25    // Give $(toVoter) the right to vote on this ballot.
26    // May only be called by $(chairperson).
27    function giveRightToVote(address toVoter) public {
28        if (msg.sender != chairperson || voters[toVoter].voted) return;
29        voters[toVoter].weight = 1;
30    }
31}
```

Development Tools (Right Panel):

- Compile, Run, Settings, Analysis, Debugger, Support tabs.
- Environment settings: Account (0xdb3..8ce11), Gas limit (3000000), Value (3000000) in wei.
- Deploy section: Ballot contract deployed at address 0xdb328861570cb95c3c6ce99bf68282.
- Transactions recorded: 3 (Details: Ballot creation, giveRightToVote, and a pending vote).
- Deployed Contracts: Ballot contract listed twice.
- Logs (Bottom):
 - transact to Ballot.vote pending ...
 - transact to Ballot.giveRightToVote errored: Error encoding arguments: Error: invalid address (arg="", type="string", value "")
 - transact to Ballot.giveRightToVote pending ...

Good things for Blockchain Developers



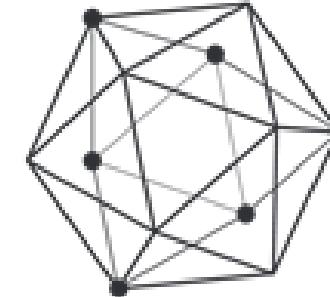
The screenshot shows the Etherscan contract overview page for the address 0x8d12A197cB00D4747a1fe03395095ce2A5CC6819. The page includes a navigation bar with links for HOME, BLOCKCHAIN, TOKENS, RESOURCES, and MORE. A search bar at the top right allows searching by Address / Txhash / Block / Token / Ens, with a 'GO' button. Below the navigation is a breadcrumb trail: Home / Accounts / Address. A sponsored banner for Color is visible. The main content area displays the Contract Overview for EtherDelta_2, showing a balance of 24,760.541107570410731904 Ether and an ether value of \$7,098,847.14. It lists 10222488 transactions. On the right, there are sections for Misc (Address Watch, Contract Creator, Token Balances), a warning about potential compiler bugs, and a section for Contract Source Code Verified (Exact match). The source code is shown in a red-bordered box:

```
11     assert(c >= a);
12     return a - b;
13 }
14
15 function safeAdd(uint a, uint b) internal returns (uint) {
16     uint c = a + b;
17     assert(c>=a && c>=b);
18     return c;
19 }
20
21 function assert(bool assertion) internal {
22     if (!assertion) throw;
23 }
```

One more thing



Quorum



HYPERLEDGER



One more thing

Seguro | <https://stockmind.io/es/#footer>

OPEN CALL STOCKMIND CARACTERÍSTICAS CASOS DE USO API CONTACTO



ESTO ES STOCKMIND

Stockmind es una plataforma de tokenización Blockchain para crear increíbles casos de uso. Descarga y despliega Stockmind en tu propia infraestructura y construye casos de uso consumiendo un sencillo API. (*)

Stockmind es un proyecto que nace desde la dirección de innovación de Bankia. Esto significa que, por ahora, sólo estamos ofreciendo la plataforma para el desarrollo de prototipos. (*)

(*) Bankia se reserva el derecho de autorizar el acceso a la API, y no se hace responsable de la administración y gestión de los tokens generados.

CREAR Y ENVIAR TOKENS ERC20

Creemos que los tokens son una revolución que facilitan el intercambio de bienes y servicios que deberían estar disponibles para cualquier desarrollador sin complicaciones. Por ello, crear tokens ERC20 en Stockmind es tan sencillo como realizar una búsqueda en Google. Sólo debes consumir un API indicando las características del token, así como por ejemplo, el número de unidades que se crearán o su descripción.



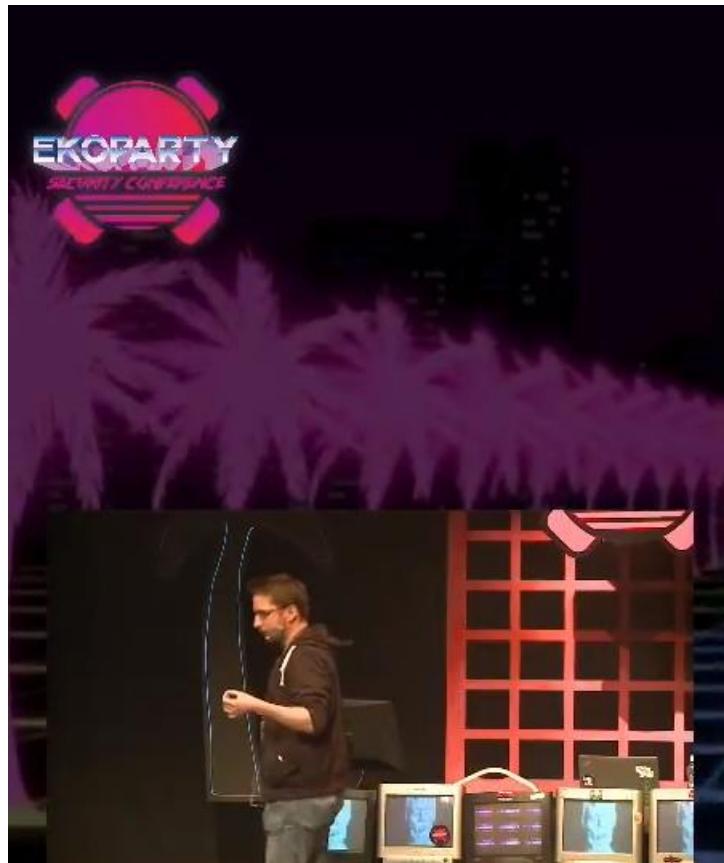
Plataforma Stockmind



One more thing



One more thing



Smart Contract Vulnerabilities

TRAIL
BITS

- “Classic” vulnerabilities:
 - Integer overflow/underflow
 - Race condition
- Logic vulnerabilities / errors in the design
 - Harder to find, but deadly

24

AUTOMATIC BUGFINDING FOR THE BLOCKCHAIN
FELIPE MANZANO & JOSSELIN FEIST



One more thing

The screenshot shows the homepage of the Black Hat Europe 2018 website. At the top right, there is a red-bordered box containing the event details: "DECEMBER 3-6, 2018" and "EXCEL LONDON / UNITED KINGDOM". Below this, a navigation bar includes links for ATTEND, TRAININGS, BRIEFINGS, ARSENAL, FEATURES, SCHEDULE, BUSINESS HALL, SPONSORS, and PROPOSALS. A "REGISTER NOW" button is also visible. In the center, a course listing for "Intro To Hacking Smart Contracts" by Mick Ayzenberg is highlighted with a red border. The course starts on December 3rd and ends on December 4th. Three pricing options are shown: EARLY (£2,599, ends Oct 5 23:59 BST), REGULAR (£2,899, ends Dec 2 23:59 GMT), and LATE (£3,099, ends Dec 6 23:59 GMT). On the left, a sidebar titled "ON THIS PAGE" lists several sections: PRICING, OVERVIEW, WHO SHOULD TAKE THIS COURSE, STUDENT REQUIREMENTS, WHAT STUDENTS SHOULD BRING, WHAT STUDENTS WILL BE PROVIDED WITH, and TRAINERS. The "WHAT STUDENTS WILL BE PROVIDED WITH" section is also highlighted with a red border. The "OVERVIEW" section contains a detailed description of the course's purpose and focus.

REGISTER NOW

DECEMBER 3-6, 2018
EXCEL LONDON / UNITED KINGDOM

ATTEND TRAININGS BRIEFINGS ARSENAL FEATURES SCHEDULE BUSINESS HALL SPONSORS PROPOSALS

BACK TO TRAINING

Intro To Hacking Smart Contracts
MICK AYZENBERG - SECURITY INNOVATION | DECEMBER 3 - 4

EARLY
£2,599
ENDS OCT. 5 23:59 BST

REGULAR
£2,899
ENDS DEC. 2 23:59 GMT

LATE
£3,099
ENDS DEC. 6 23:59 GMT

ON THIS PAGE

PRICING

OVERVIEW

WHO SHOULD TAKE THIS COURSE

STUDENT REQUIREMENTS

WHAT STUDENTS SHOULD BRING

WHAT STUDENTS WILL BE PROVIDED WITH

TRAINERS

Overview

As Blockchain platforms become more and more developed, many companies are beginning to investigate how this emerging technology might affect their business. In this two day course we dive deep into state of the art methodologies used when developing smart contracts for Blockchain enabled Decentralized Applications (DApps). We focus the training on the Ethereum Blockchain and the Solidity language, as these are currently the most used platforms for building decentralized applications. The course will be a tutorial that guides participants through Solidity and its constructs so that students will be capable of developing these applications themselves, and identifying the most common vulnerabilities on this platform.

Questions?



Thanks!

Email: **vicsanjinez@gmail.com**

Twitter: **@victorsanjinez**

Github: **<https://github.com/vicsanjinez>**

