

# Curso desarrollo Blockchain Ethereum con Solidity

Clase 1

# Introducción a Ethereum

# Introducción a Ethereum

- Ethereum es una Plataforma descentralizada que permite la creacion de acuerdos inteligentes (Smart Contracts)
- ¿ Que es un Smart Contract? Es un conjunto de promesas, especificadas en formato digital, que incluyen protocolos que los participantes podrán ejecutar sobre dichas promesas.
- Es decir, en palabras simples, un SmartContract es un programa distribuído.
- Lo cierto es que hasta la aparición de las blockchains, no fue posible implementar esta idea dado que se requiere de un sistema financiero que lo soporte, junto con la infraestructura de transacciones programables.
- Con los SmartContracts, en base a una serie de entradas, se pueden ejecutar transacciones, hacer pagos, intercambiar VALOR.



# Bitcoin White Paper & ¿Porqué no desarrollamos sobre bitcoin?

# Bitcoin & Ethereum White Paper

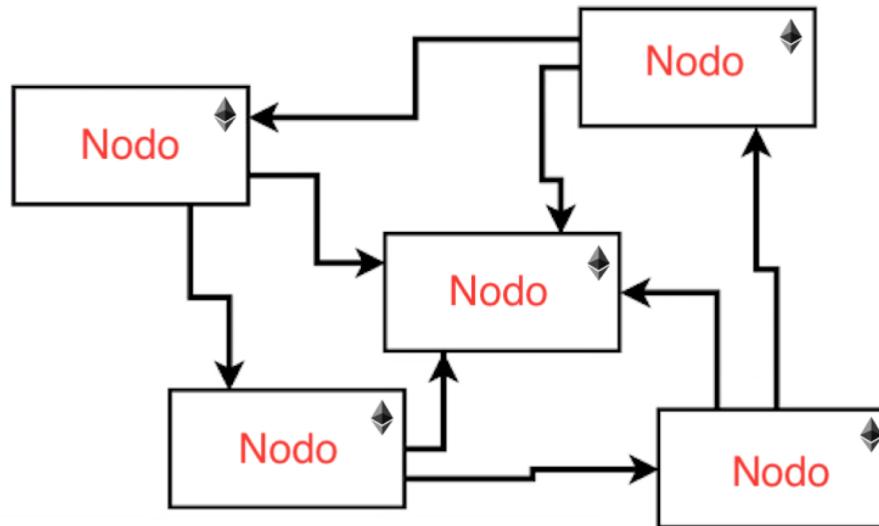
- 31 de Octubre de 2008 - Bitcoin WhitePaper
- Es descrito como un sistema de pagos peer to peer sin intermediarios, es decir sin bancos (Peer to Peer Electronic Cash System)
- Diciembre de 2013 - "Ethereum Whitepaper"
- Se discute sobre la necesidad de tener más control programático sobre las transacciones
- Se introduce la idea de Contratos Inteligentes como una entidad que puede enviar y recibir monedas.
- BTC WhitePaper: <https://bitcoin.org/bitcoin.pdf>
- ETH Paper:<http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html>



# Interfaceando con las Ethereum Networks

# Interfaceando con las Ethereum Networks

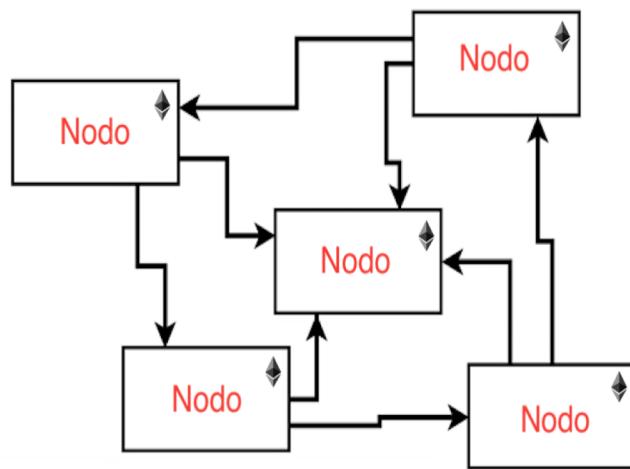
- Son usadas para transferir \$ y almacenar data
- Cualquiera puede correr un Nodo de Ethereum
- Existen muchas redes diferentes de Ethereum
- Las redes pueden estar formadas por uno o más nodos
- Cada nodo contiene una copia completa de la blockchain de Ethereum



# Interfaceando con las Ethereum Networks

A la hora de trabajar contra las redes de Ethereum, hay principalmente 2 grupos de tecnologías con las que contaremos

DEVELOPERS



USUARIOS



# ¿Qué es el Ether?

# ¿Qué es el Ether?

- El Ether es la moneda utilizada en la Ethereum Blockchain. Sirve como medio de pago para los SmartContracts y también como almacén de valor.
- Un Ether que se puede dividir hasta en 18 decimales
- No hay límite en la cantidad de unidades de ether que pueden ser liberadas\*
- Es muy importante tener en cuenta que los SmartContracts trabajarán en WEI, ya que al momento los decimales no son soportados por la EVM.



# ¿Qué es el Ether?

El Ether, al igual que cualquier otro criptoactivo, posee fluctuaciones constantes que pueden verse como en el siguiente gráfico.



# Metamask

# Metamask

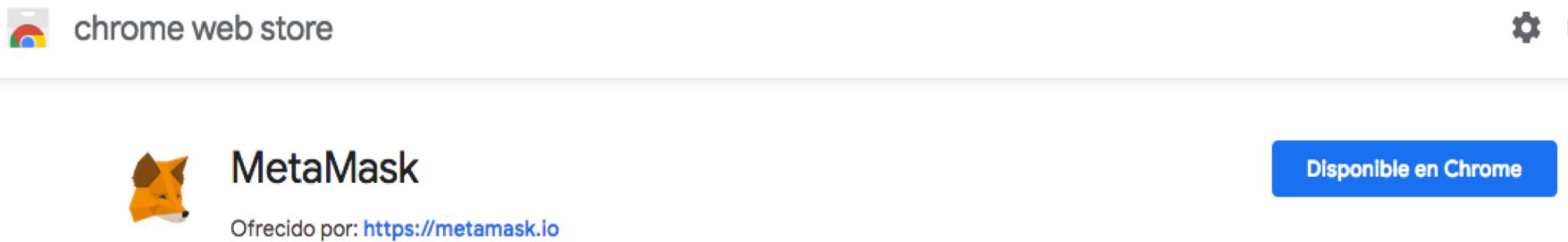
- Metamask es un módulo de Chrome que usa una serie de nodos para realizar las operaciones que necesitemos.
- Nos permite enviar y recibir información
- Nos permite enviar y recibir “dinero”
- Nos permite enviar y recibir “data”
- Ether ilimitados\*\*



# Metamask

Pasos para la instalación

- Abrir Chrome
- Abrir el web store
- Buscar Metamask
- Agregar a Chrome
- Agregar Extensión
- Listo!



# Metamask

Pasos para la configuración inicial

- Abrir Metamask
- Aceptar los términos y condiciones
- Setear una clave\*
- Guardar de manera segura la clave de restore
- Listo!



# Metamask

Al completar la configuración han pasado las siguientes cosas

1. Se ha creado un Account Address (0xcf....)
2. Se ha generado una Public Key
3. Se ha generado una Private Key
4. Ya podemos operar sobre la Blockchain!



A screenshot of the Metamask mobile application interface. At the top, it says "Try the New MetaMask Now or Learn More". Below that, there's a profile icon, a "Rinkeby Test Net" dropdown, and a settings menu. The main area shows "Account 1" with the address "0x3a7D7...". It displays 40.502 ETH and 8450.74 USD. There are "BUY" and "SEND" buttons. Below this, there are tabs for "SENT" and "TOKENS", with "TOKENS" currently selected. A message at the bottom states "No transaction history."

# Enviando / recibiendo Ether

# Enviando / recibiendo Ether

Metamask posee dos interfaces para su utilización. Actualmente la de la izquierda es la estable y la de la derecha es la BETA.

En cualquiera de las dos basta con presionar el botón "SEND" para enviar Ether a una dirección dentro de la Ethereum Blockchain

The screenshot shows the stable version of the MetaMask interface. At the top, there's a blue bar with the text "Try the New MetaMask Now or Learn More". Below it, a navigation bar includes a fox icon, a "Rinkeby Test Net" dropdown, and a three-dot menu. The main area features a circular profile picture for "Account 1" (0x3a7D7...) and a balance of "40.502 ETH" equivalent to "\$8,450.74 USD". There are "BUY" and "SEND" buttons. Below these are tabs for "SENT" and "TOKENS", with "SENT" currently selected. A message "No transaction history." is displayed. The background is white with orange and grey accents.



The screenshot shows the BETA version of the MetaMask interface. It has a similar layout to the stable version but with some differences. The top bar includes a fox icon, a dropdown for "Red privada Rinkeby", and a circular profile picture for "Account 1" (0x3a7D...c25a). Below this is a "DETALLES" button. The main area shows the balance "40.502 ETH" and its value in USD. At the bottom is a "AGREGAR TOKEN" button. The overall design is more modern and minimalist compared to the stable version.

# Enviando / recibiendo Ether

Al presionar SEND, se nos pedirá una dirección de envío (que puede ser cargada o escaneada por QR) y una cantidad de Ether a enviar.

**Enviar Ether** ×

Sólo envía a una dirección de Ethereum

De:: Account 1  
113.431895 ETH  
\$24,846.12 USD

Para: 0x98d1F051B6c7b2Afc3F0cQR

Cantidad: 1.4 ETH  
\$306.66 USD

Max

Comisión de gas: 0.000021 ETH  
\$0.00 USD ≡

CANCELAR SIGUIENTE

# Block Time

# Block Time

Es la cantidad de tiempo que toma ejecutar esos cientos de miles de diferentes posibles hashes hasta encontrar el valor que actualmente sea igual al que buscamos

DATA	+	NONCE	=	OUTPUT HASH	OH BASE 10	En el target? (<1000)
Lorem ipsum	+	0	=	a23042b2e	178917215	NO
Lorem ipsum	+	1	=	cbc1491	29589283	NO
Lorem ipsum	+	2	=	0ca24258	94869869	NO
Lorem ipsum	+	3	=	d9eed91	13938166	NO
Lorem ipsum	+	4	=	1488baec	419386918	NO
Lorem ipsum	+	5	=	0077bbb	100	SÍ

Tiempo en encontrar la solución

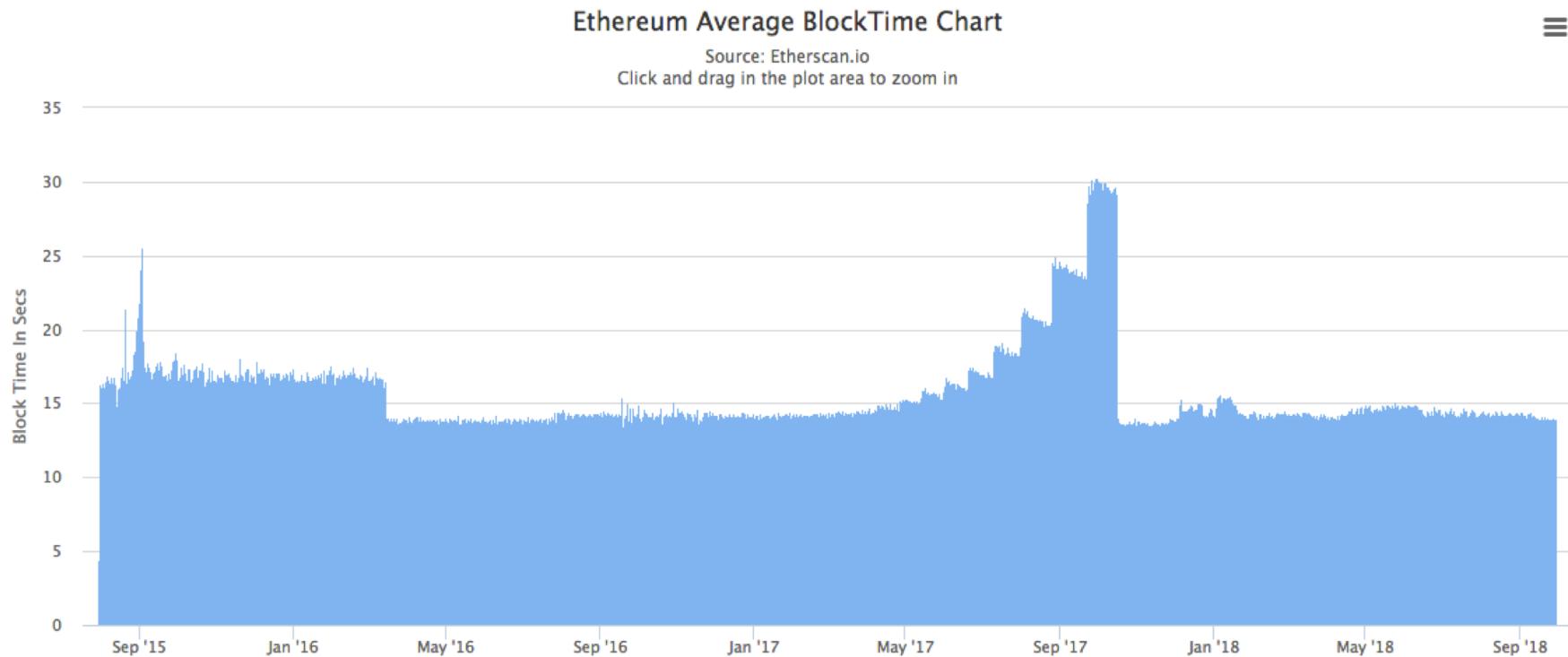
==

**BLOCK TIME**

OH = Output Hash

# Block Time

Se puede ver el tiempo estimado actual en <https://etherscan.io/chart/blocktime>



# WEI

# WEI

- Es la 1/18 parte de un Ether
- $1 \text{ ETH} = 10^{18} \text{ WEI}$  ( $1 \text{ ETH} = 1000000000000000000 \text{ WEI}$ )
- Su finalidad es la de subdividir una unida de Ether
- Existen multiples conversiones a distintas unidades
- Los smartContracts operan en WEI y NO en Ether



Wei	1000000000000000000000000
Kwei, Ada, Femtoether	1000000000000000000000000
Mwei, Babbage, Picoether	100000000000000000000000
Gwei, Shannon, Nanoether, Nano	10000000000000000000000
Szabo, Microether,Micro	1000000
Finney, Milliether,Milli	1000
Ether	1
Kether, Grand,Einstein	0.001
Mether	0.000001
Gether	0.000000001
Tether	0.000000000001
<b>USD(at 224.172\$ p/ ether)</b>	<b>224.172</b>
<b>EUR(at 194.526€ p/ ether)</b>	<b>194.526</b>

# Gas

# GAS

- El gas podemos decir que es el precio de las transacciones en los contratos de Ethereum
- Para hacer una analogía, sería como los KiloWatts para contar el gasto de electricidad. Es el costo por ejecutar algo.
- El gas podemos decir que es el precio de las transacciones en los contratos de Ethereum.
- En teoría, el GAS sirve para desacoplar el precio del Ether al de la ejecución de contratos dado que el GAS tiene de por sí, un precio en Ether.
- El gas podemos decir que es el precio de las transacciones en los contratos de Ethereum.
- El mismo dependerá de las operaciones que ejecute.
- Al ejecutar una transacción sobre un contratos, fijaremos el precio GAS que estamos dispuestos a pagar, cuanto mas gas, mayor será la prioridad de nuestra transacción en la blockchain ya que los mineros tomarán primero las transacciones más lucrativas.
- Supongamos que crear un contrato cuesta hoy unos 32000 GAS. Si le ponemos un precio de 25 gwei tenemos que la transaccion nos costará  $0.008 \text{ ETH}$  ( $32000 * 25 / 10^8$ )



# GAS

Existe un documento público donde se indica el costo de GAS según las operaciones realizadas.

El mismo se encuentra en

[https://docs.google.com/spreadsheets/d/1n6mRqkBz3iWcOIRe\\_mO09GtSKEKrAsfO7Frgx18pNU/edit#gid=0](https://docs.google.com/spreadsheets/d/1n6mRqkBz3iWcOIRe_mO09GtSKEKrAsfO7Frgx18pNU/edit#gid=0)

Gas Costs from Yellow Paper – EIP-150 Revision (1e18248 - 2017-04-12)

Archivo Editar Ver Insertar Formato Datos Herramientas Complementos Ayuda

100% Solo ver

Value

1	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes	Formula	Formula Notes				
2	0x00	STOP		0 zero		0	0 Halts execution.						
3	0x01	ADD		3 verylow		2	1 Addition operation.						
4	0x02	MUL		5 low		2	1 Multiplication operation.						
5	0x03	SUB		3 verylow		2	1 Subtraction operation.						
6	0x04	DIV		5 low		2	1 Integer division operation.						
7	0x05	SDIV		5 low		2	1 Signed integer division operation (truncated).						
8	0x06	MOD		5 low		2	1 Modulo remainder operation						
9	0x07	SMOD		5 low		2	1 Signed modulo remainder operation.						
10	0x08	ADDMOD		8 mid		3	1 Modulo addition operation.						
11	0x09	MULMOD		8 mid		3	1 Modulo multiplication operation.						
12	0xa	EXP	FORMULA			2	1 Exponential operation. (exp == 0) ? 10 : If exponent is 0, gas used is 10. If exponent is greater than 0, gas used is 10 plus 10 times a factor related to how large the log of the exp						
13	0xb	SIGNEXTEND		5 low		2	1 Extend length of two's complement signed integer.						
14	0x10	LT		3 verylow		2	1 Less-than comparison.						
15	0x11	GT		3 verylow		2	1 Greater-than comparison.						
16	0x12	SLT		3 verylow		2	1 Signed less-than comparison.						
17	0x13	SGT		3 verylow		2	1 Signed greater-than comparison.						
18	0x14	EQ		3 verylow		2	1 Equality comparison.						
19	0x15	ISZERO		3 verylow		1	1 Simple not operator.						
20	0x16	AND		3 verylow		2	1 Bitwise AND operation.						
21	0x17	OR		3 verylow		2	1 Bitwise OR operation						
22	0x18	XOR		3 verylow		2	1 Bitwise XOR operation.						
23	0x19	NOT		3 verylow		1	1 Bitwise NOT operation.						
24	0x1a	BYTE		3 verylow		2	1 Retrieve single byte from word						
25	0x20	SHA3	FORMULA			2	1 Compute Keccak-256 hash. 30 + 6 * (size of i) 30 is the paid for the operation plus 6 paid for each word (rounded up) for the input data.						
26	0x30	ADDRESS		2 base		0	1 Get address of currently executing account.						



# Transacciones

# Transacciones

Una transacción es un registro de una operación realizada sobre la blockchain

TxHash:	0x5ef89b69f368b87fb1440696e999fda567d75e14ae06789a6533e25e3d836704
TxReceipt Status:	Success
Block Height:	<a href="#">6349486</a> (78334 Block Confirmations)
TimeStamp:	12 days 21 hrs ago (Sep-17-2018 05:00:55 PM +UTC)
From:	<a href="#">0xa1ab7a4aa264745912db261536291336f7e543ac</a>
To:	<a href="#">0xfaff7cda4f7cd01675e82c006c0f8d6ba276fc86</a>
Value:	0.3339 Ether (\$78.69)
Gas Limit:	4000000
Gas Used By Transaction:	21000
Gas Price:	0.000000005 Ether (5 Gwei)
Actual Tx Cost/Fee:	0.000105 Ether (\$0.02)
Nonce & {Position}:	679   {20}

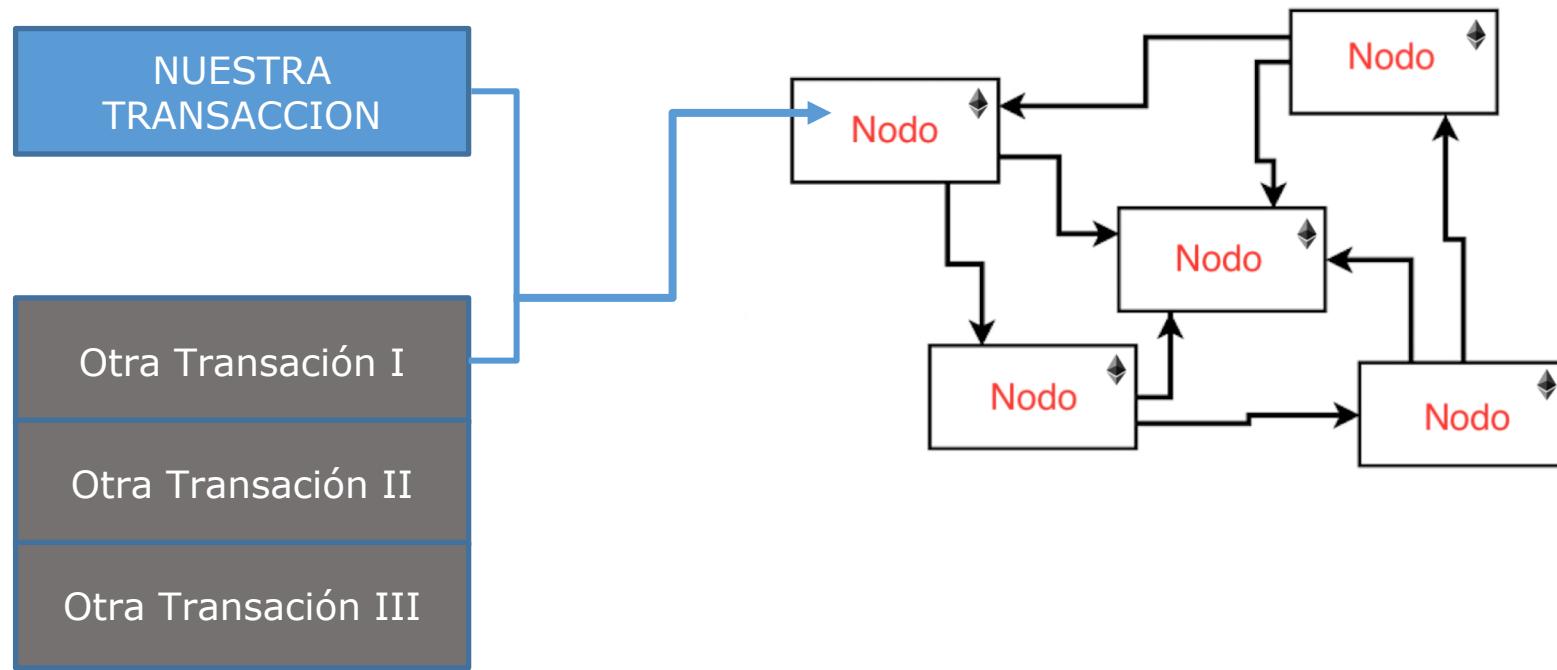
# Transacciones

Toda transacción tiene multiples propiedades. Entre las más importante se encuentran las siguientes

Nonce	Cuantas veces el sender(remitente) ha enviado una transacción
To	Address a donde estará llegando el Ether enviado
Value	Cantidad de Ether que se está enviando al "To"
gasPrice	Cantidad de Ether que quien envía está esperando pagar por unidad de GAS para que esta transacción sea procesada
startGas / gasLimit	Unidades de gas que la transacción puede consumir
v	Parte criptográfica de información que puede ser utilizada para generar la dirección (Address) de quien envía el Ether.
r	Idem anterior
s	Idem anterior

# Transacciones

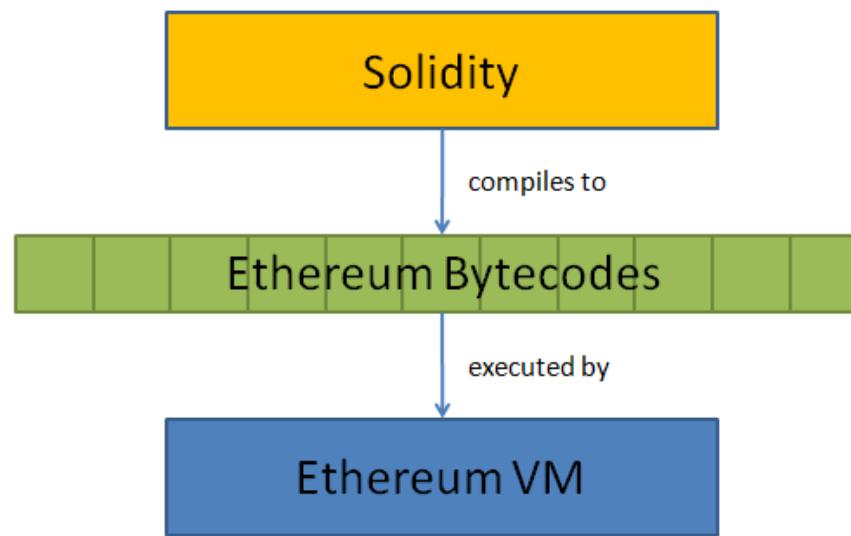
Es importante aclarar que cuando enviamos una transacción a la blockchain, en realidad la estaremos enviando a un nodo particular y no al conjunto (EN)



# EVM (Ethereum Virtual Machine)

# Ethereum Virtual Machine

- La EVM es la que soporta realmente la ejecución de los smart contracts.
- Al estar estandarizada, pueden existir muchísimas implementaciones diferentes siempre que soporten las operaciones definidas. (por ej. GETH y Parity).
- La EVM trabaja en un lenguaje intermedio, es decir, trabaja en Bytecode.
- Cuando programamos para la blockchain, podemos hacerlo en diferentes lenguajes, da igual ya que finalmente compilarán a Bytecode que es lo que realmente entiende la EVM.



# Solidity vs Phyton vs Viper vs LLL - Tendencias

# Solidity vs Phyton vs Viper vs LLL - Tendencias

- Solidity es el lenguaje que podríamos decir es el estándar para el desarrollo de SmartContracts.
- No es el único, existen otros como Phyton, LLL, Serpent, Viper, etc.
- Solidity es verdaderamente sencillo, su sintaxis es similar a javascript (se ha tomado parte de la sintaxis ECMASCIPT) pero a la vez es diferente (Solidity, a diferencia de JavaScript, es tipado).
- Solidity no solo sirve para Ethereum, sino para otras Blockchains como Rootstock o Tendermint.
- Phyton, Serpent y Viper tienen una sintaxis similar



# Estructura básica de un contrato inteligente

# Estructura básica de un contrato inteligente

Vamos a <http://remix.ethereum.org>

```
« + browser/ballot_test.sol ×
1 pragma solidity ^0.4.7;
2 import "remix_tests.sol"; // this import is automatically injected by Remix.
3 import "./ballot.sol";
4
5 contract test3 {
6
7     Ballot ballotToTest;
8     function beforeAll () {
9         ballotToTest = new Ballot(2);
10    }
11
12     function checkWinningProposal () public {
13         ballotToTest.vote(1);
14         Assert.equal(ballotToTest.winningProposal(), uint(1), "1 should be the winning proposal");
15    }
16
17     function checkWinninProposalWithReturnValue () public constant returns (bool) {
18         return ballotToTest.winningProposal() == 1;
19    }
20 }
```