

# Usos y Aplicaciones de la Tecnología Blockchain

---

Francisco Rosales Marticorena, PhD.

[francisco.rosales-marticorena@protonmail.com](mailto:francisco.rosales-marticorena@protonmail.com)

22.09.18 – 06.10.18

ESAN Graduate School of Business

## Tabla de Contenidos:

- 1** Introducción
- 2** Conceptos Básicos
- 3** Blockchains Públicas
- 4** Una moneda en C++
- 5** Evaluación 1
- 6** Una Moneda en Solidity
- 7** Blockchains Privadas
- 8** Esquemas Ponzi y Pirámides
- 9** Retos y Preguntas Abiertas
- 10** Evaluación 2

# Introducción

---

# Datos Generales del Curso

**Asignatura:** Usos y Aplicaciones de la Tecnología Blockchain

**Área académica:** Programa de Especialización para Ejecutivos

**Año y semestre:** 2018 – II

**Profesor:** Francisco Rosales Marticorena, PhD.  
Mail: francisco.rosales-marticorena@protonmail.com  
Teléfono: 947-147-405

**Materiales:** <https://github.com/PhiChain/PHICoin>

# Sumilla

Este curso es una introducción a la tecnología Blockchain y las monedas criptográficas mediante la presentación de casos reales de estudio.

# Objetivos de la Asignatura

Al terminar el curso, el estudiante estará en capacidad de:

- Explicar qué es la tecnología blockchain, por qué es una tecnología disruptiva, y describir los conceptos básicos asociados a ella.
- Enumerar las diferencias entre una blockchain pública y una privada; y brindar ejemplos de ambos tipos de blockchain.
- Identificar los principales peligros y retos de la tecnología blockchain en términos de adopción y regulación.

# Programación de Contenidos

- 1 Introducción a la Tecnología Blockchain:**
  - Sesión 1: Introducción y conceptos básicos
  - Sesión 2: Otros conceptos necesarios
- 2 Blockchains Públicas y Privadas:**
  - Sesión 3: Blockchains públicas
  - Sesión 4: Una moneda en C++
  - Sesión 5: Primera evaluación
  - Sesión 6: Una moneda en Solidity
  - Sesión 7: Blockchains privadas
- 3 Riesgos y Futuro de Blockchain:**
  - Sesión 7: Esquemas Ponzi y pirámides
  - Sesión 9: Retos y preguntas abiertas
  - Sesión 10: Segunda evaluación

# Metodología

El curso tiene carácter teórico-práctico, las exposiciones del profesor se complementarán con actividades que harán los alumnos en el salón de clase, y fuera de él. Las principales actividades son:

- Participar en clase.
- Leer la bibliografía indicada en el programa.
- Rendir las evaluaciones programadas.

# Evaluación

El curso tendrá dos evaluaciones:

- Evaluación individual: 22 de septiembre (sesión 5)
- Evaluación grupal: 6 de octubre (sesión 10)

La nota final será calculada como:

$$\text{nota final} = 0.4 \times (\text{eval individual}) + 0.6 \times (\text{eval grupal}),$$

los grupos deben ser de máximo 4 personas.

## Fuentes de Información

- [AA1] Antonopoulos, A. (2017). The Internet of Money: Vomen 1. Merkle Bloom LLC.
- [AA2] Antonopoulos, A. (2017). The Internet of Money: Volumen 2. Merkle Bloom LLC.
- [CD] Dannen, C. (2017). Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Brooklyn, New York. USA.
- [HD] Diedrich, H. (2016). Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations. Ethereum Foundation.
- [AN] Narayanan, A., J. et al. (2016). Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction. Princeton University Press.

# Docente: Francisco Rosales Marticorena, PhD.

## Educación:

- Doctor. Matemáticas y Ciencia Comp. Universidad de Göttingen.
- Magister. Matemáticas Ap. y Estadística. SUNY Stony Brook.
- Magister. Matemáticas. PUCP.
- Licenciado y Bachiller. Economía. UP.

## Experiencia:

- 2018– presente: Gerente de Servicios Financieros. EY Perú.
- 2017–2018: Profesor investigador. Dep. de Finanzas. UP.
- 2011–2016: Investigador asociado. Instituto de Matemática Estocástica. Universidad de Goettingen.
- 2005–2008: Científico. CGIAR en CIP.

**Desarrollo:** Creación de una moneda criptográfica. Fork de LearnCoin (fork de LTC (fork de BTC)). Talleres: UP, UTEC, UNI, ESAN, UPC.

## Asistentes:

- Expectativa: ¿techie, ejecutivo?
- Sectores: ¿startups, privado, público, reguladores?
- ¿Qué les gustaría llevarse del curso?

# Programa 22.09.18

Sesión	Inicio	Fin	Tópico
1	08:30	10:00	Intro & conceptos básicos
2	10:30	12:00	Blockchain públicas
3	13:30	15:00	Blockchain públicas (cont.)
4	15:15	16:45	Una moneda en C++
5	16:45	18:15	Evaluación Individual

## **Conceptos Básicos**

---

## Ejemplo 2.1 (El Problema de los Amigos)

Considere una economía formada por Usted y sus amigos: Alice, Bob y Charlie. Ustedes realizan actividades por las que se debe pagar con dinero, pero en ocasiones algunos de sus amigos no tienen efectivo, y otro debe cubrir el costo. Para llevar las cuentas claras deciden abrir una página web con un libro mayor para registrar las deudas y saldarlas luego.

### Protocolo:

- Cualquiera puede agregar líneas en el libro mayor.
- Al final de cada mes todos se reúnen y pagan sus deudas en efectivo.

### Problema:

Confianza. Si cualquiera puede agregar líneas en el libro mayor, es posible falsear deudas, e.g. Charly puede agregar una deuda (falsa) de Alice.

## Definición 2.1 (Firma Digital)

Es una verificación digital que garantiza que su dueño ha visto la transacción y la autoriza. Para que un usuario tenga una firma digital, debe contar con una clave pública (CP) y una clave privada (CS).

### Nota 2.1

La firma digital es “más segura” que la firma física en tanto cambia para distintos mensajes. En particular, considere:

$$\mathcal{F}(\text{Mensaje}, CS) = \text{firma}$$

$$\mathcal{V}(\text{Mensaje}, \text{firma}, PS) = \text{True/False},$$

donde  $\mathcal{F}(\cdot, \cdot)$  es la función que construye la firma digital, y  $\mathcal{V}(\cdot, \cdot)$  es la función que verifica que la firma es legítima.

## Nota 2.2

Aunque un ataque de fuerza bruta para encontrar firma tal que  $\mathcal{V}(\text{Mensaje}, \text{firma}, \text{CP}) = \text{True}$ , es posible, es muy difícil, e.g. si firma tiene 256 bits, el ataque puede recorrer  $2^{256}$  casos.

## Nota 2.3

Note que si cada uno de sus amigos usa una firma digital, se puede estar seguro de que las deudas son legítimas. Sin embargo aún hay un problema, pues es posible copiar una misma línea varias veces. Este problema se resuelve agregando un contador a cada mensaje.

### Protocolo:

- Cualquiera puede agregar líneas en el libro mayor.
- Al final de cada mes todos se reúnen y pagan sus deudas en efectivo.
- Sólo las transacciones firmadas son válidas.

### Problema:

Confianza. Todos deben honrar sus deudas al final del mes.

## Nota 2.4

*Dado que sólo los deudores deben cancelar sus deudas en efectivo, es posible garantizar que no habrá deudores si ninguno de los amigos puede tener un saldo negativo (asumiendo que el libro mayor inicia con un saldo positivo  $M_j > 0$  para cada amigo  $j \in \{A, B, C, X\}$ ).*

### Protocolo:

- Cualquiera puede agregar líneas en el libro mayor.
- Sólo las transacciones firmadas son válidas.
- No saldos negativos.

### Problema:

Confianza. El libro mayor es centralizado si e.g. está en una página web, i.e. es vulnerable.

## Definición 2.2 (Libro Mayor Distribuído)

*Es un libro mayor descentralizado que se actualiza en múltiples nodos de una red (e.g. los amigos) al mismo tiempo.*

### Problema:

*¿Cómo saber que todos los nodos de la red están actualizando lo mismo?*

### Solución:

- Crear incentivos para validadores de libros mayores.
- Si hay dos libros mayores validados y distintos, confiar en el que ha sido más veces validado.

# Funciones Hash Criptográficas

## Definición 2.3 (Función Hash)

Una función hash es  $f : \mathbb{X} \rightarrow \mathbb{Y}$ , donde  $\mathbb{X}$  contiene cadenas de texto, o archivos, e  $\mathbb{Y}$  es una cadena de cierta longitud. Además pequeños cambios en  $x \in \mathbb{X}$  generan grandes cambios en  $f(x)$ .

## Ejemplo 2.2 (SHA256)

En este caso la imagen de  $f$  tiene 256 dígitos.

$SHA256("arakata") \neq SHA256("Arakata") \neq SHA256("arakat4")$ .

## Definición 2.4 (Función Hash Criptográfica)

Es una función hash en la que la pre-imagen es muy difícil de calcular, i.e. la mejor opción es buscar en todo  $\mathbb{X}$ .

## Definición 2.5 (Proof-of-Work)

*Proof-of-Work es el trabajo por el que los validadores de los bloques son recompensados. El trabajo consiste en encontrar una cadena numérica (nonce), tal que*

$$\text{SHA256}(LM, \text{nonce}) = \underbrace{0 \dots 0}_{n \text{ ceros}} \# \dots \#,$$

*donde  $LM$  representa la información contenida en el libro mayor, y  $n$  es el número de ceros con el que empieza la imagen de la función hash. Si  $n = 30$ , se deben explorar  $2^{30}$  casos . La prueba de trabajo es el nonce.*

## Nota 2.5

*Los validadores de los bloques son llamados “mineros”. Actualmente su recompensa es de 12.5 BTC por bloque minado. Esta recompensa es el mecanismo por el cual la blockchain hace emisión monetaria.*

De “libros mayores” a “bloques”:

- Considere el problema de los amigos.
- Suponga que al final del primer día se juntan todas las transacciones en un libro mayor (bloque): “Bloque 1”, y que a este bloque se le aplica una prueba de trabajo, de modo que es validado.
- Considere el mismo problema el siguiente día, pero adicionando en el encabezado del nuevo bloque “Bloque 2”, el hash correspondiente al último bloque validado, i.e. el “Bloque 1”, etc.

## Nota 2.6

*El conjunto bloques encadenados se denomina Blockchain. Es el libro mayor con una estructura que permite actualizarlo por bloques.*

## Nota 2.7

*Note que es posible que dos (o más) Blockchains coexistan en un mismo momento. En este caso el sistema espera y toma como verdadera a la Blockchain más larga, i.e. la cadena de bloques en la que se ha invertido mayor poder computacional.*

## Nota 2.8

*En Bitcoin el número  $n$  que se requiere para minar un bloque cambia periódicamente de manera que el tiempo requerido para minar un bloque es siempre de 10 minutos. Para Ethereum es 15 segundos, para XRC 3.5 segundos y para LTC 2.5 minutos.*

## Nota 2.9

*La recompensa de los mineros es la única forma de emitir bitcoin, y se reduce de acuerdo a una progresión geométrica que garantiza que la masa monetaria de bitcoin es 21M. Último bitcoin en 2140.*

## Definición 2.6 (El Problema de los Generales Bizantinos)

*El Problema de los Generales Bizantinos es la dificultad que enfrentan dos sistemas cuando uno de ellos intenta comunicarse con el otro sin que el mensaje sea corrompido.*

Solución: Hacer que corromper el mensaje sea muy difícil. La idea es que el receptor imponga la condición:

$$f(\text{mensaje}, \text{nonce}) = \underbrace{0 \dots 0}_{n \text{ ceros}} \# \dots \#,$$

para considerar al mensaje “mensaje”, como válido. Considere que en esta expresión, “ $f$ ” y “ $n$ ” son conocidos por el atacante y que el “nonce” debe estar adjunto al mensaje, i.e. el atacante también lo conoce.

## Generales Bizantinos: Ejemplo

### Ejemplo 2.3

Considere que  $\mathcal{A}$  quiere comunicar el mensaje “Atacar Domingo” al sistema  $\mathcal{B}$ ,  $f$  es la función criptográfica SHA256,  $n = 5$ , y  $\mathcal{A}$  ha determinado que el *nonce* que resuelve

$$f(\text{Atacar Domingo}, \text{nonce}) = 00000\# \dots \#$$

es “1r6k1t9”. Note que si el mensaje es interceptado y corrompido a “Atacar Lunes”, la condición de verificación se ha roto:

$$f(\text{Atacar Lunes}, 1r6k1t9) \neq 00000\# \dots \#$$

Es decir, para corromper la comunicación se deben alterar el “mensaje” y el “nonce”. Lo primero es inmediato, pero lo segundo es muy costoso.

## Definición 2.7 (El Problema del Gasto Doble)

*El problema del gasto doble es un falla potencial del dinero digital, por el cual el mismo token digital puede ser gastado más de una vez.*

Solución: Base de datos para el registro de transacciones (Blockchain).

## Nota 2.10 (Ataque del 51%)

*Dado que, en la presencia de un conflicto de información, la Blockchain toma la cadena más larga como verdadera. Si la mayor parte del poder computacional está concentrado en una persona, ésta puede corromper la Blockchain, y gastar dos veces el mismo token.*

## Ejemplo 2.4 (Gasto Doble)

Considere dos Blockchains idénticas: una Blockchain pública ( $BCPUB$ ) y la copia privada de un atacante ( $BCPRI$ ). Considere que el atacante tiene la mayor parte del poder computacional total, y que durante cierto intervalo de tiempo  $T$  decide minar privadamente (no anuncia en  $BCPUB$ ) todas las transacciones de  $BCPUB$ . Dado que el atacante tiene mayor poder computacional, transcurrido  $T$ ,  $BCPRI$  será más larga que  $BCPUB$ , de modo que si se sube  $BCPRI$  a la red, ésta será tomada como verdadera. El beneficio atacante es aparente si se considera que durante  $T$  éste pudo hacer compras en  $BCPUB$ , las cuales no están registradas en  $BCPRI$ , la cual ha sido tomada como verdadera por la comunidad.

### Nota 2.11

En Mayo de 2018 el ataque del 51% fue usando contra Bitcoin Gold. El atacante tuvo suficiente poder computacional como para continuar gastando doble durante tres días. [Leer artículo](#).

## Definición 2.8 (Esquemas Ponzi)

*El Esquema Ponzi es una operación fraudulenta de inversión que implica el pago de intereses a los inversores de su propio dinero invertido o del dinero de nuevos inversores. Consiste en un proceso en el que las ganancias que obtienen los primeros inversionistas son generadas gracias al dinero aportado por ellos mismos o por otros nuevos inversores.*

Esquemas Ponzi asociados a monedas criptográficas:

- Bitconnect
- Centra
- PinCoin
- Ifan
- PlexCoin
- OneCoin

# Problemas Prácticos

Re: Consulta acerca de Criptomonedas

To: [REDACTED] Cc: francisco

Hola [REDACTED]

Te contacto con el profesor Francisco Rosales para que le puedas hacer tus consultas... él es experto en criptomonedas...

Saludos!

LCB

El 19 de septiembre de 2018, 12:57, [REDACTED] escribió:

Hola [REDACTED] no conozco sobre el tema, pero te presento al Profesor [REDACTED] El está más vinculado a estos temas

Un abrazo

[REDACTED]

El mar., 18 de sep. de 2018 3:12 p. m., [REDACTED] escribió:

Estimada [REDACTED]

Buenas tardes, es muy probable que no me recuerde pero llevo el Mba 14 en Arequipa usted nos enseñó el curso de macro, recurro a usted debido a que tengo una propuesta para comprar una criptomoneda llamada Dagcoin pero esta trabaja a través de redes me mercadeo para que se masifique bajo la figura de una Universidad on Line llamada DagUniversity.

Quiero consultarle qué tan cierto es esto de las criptomonedas como monedas del futuro, su rentabilidad y en q escenario sería conveniente invertir. Cabe resaltar que el monto para entrar es mínimo 500 euros.

Quedo atenta a su respuesta.

Muchas gracias!!!

19. September 2018 at 13:58

[Details](#) 

## **Blockchains Públicas**

---

## Definición 3.1 (Bitcoin)

*Bitcoin es un protocolo y red P2P que se utiliza como moneda criptográfica, sistema de pago y depósito de valor. Su unidad de cuenta nativa se denomina bitcoin. Esas unidades son las que sirven para contabilizar y transferir valor por lo que se clasifican como moneda digital.*

Características:

- No está respaldado por ningún gobierno o banco central.
- Resuelve el problema del doble gasto utilizando un sistema de prueba de trabajo (PoW).
- Resuelve el problema de los generales bizantinos al lograr el consenso en una red no confiable.
- Las transacciones no necesitan de intermediarios.
- El protocolo es código abierto.

No es algo nuevo:

- InkaCoin existe desde el año 2013: <https://coinmarketcap.com/currencies/inkacoin/historical-data/>
- Un candidato a la presidencia del Perú propuso poner las elecciones de 2016 en blockchain:  
<https://www.criptonoticias.com/sucesos/candidato-presidencial-peru-blockchain-campana-politica/>.
- Bitinka es un exchange latinoamericano:  
<https://www.bitinka.com/pe/bitinka/home>

# Bitcoin: Perú (Cont.)

Maneras de conseguir Bitcoin:

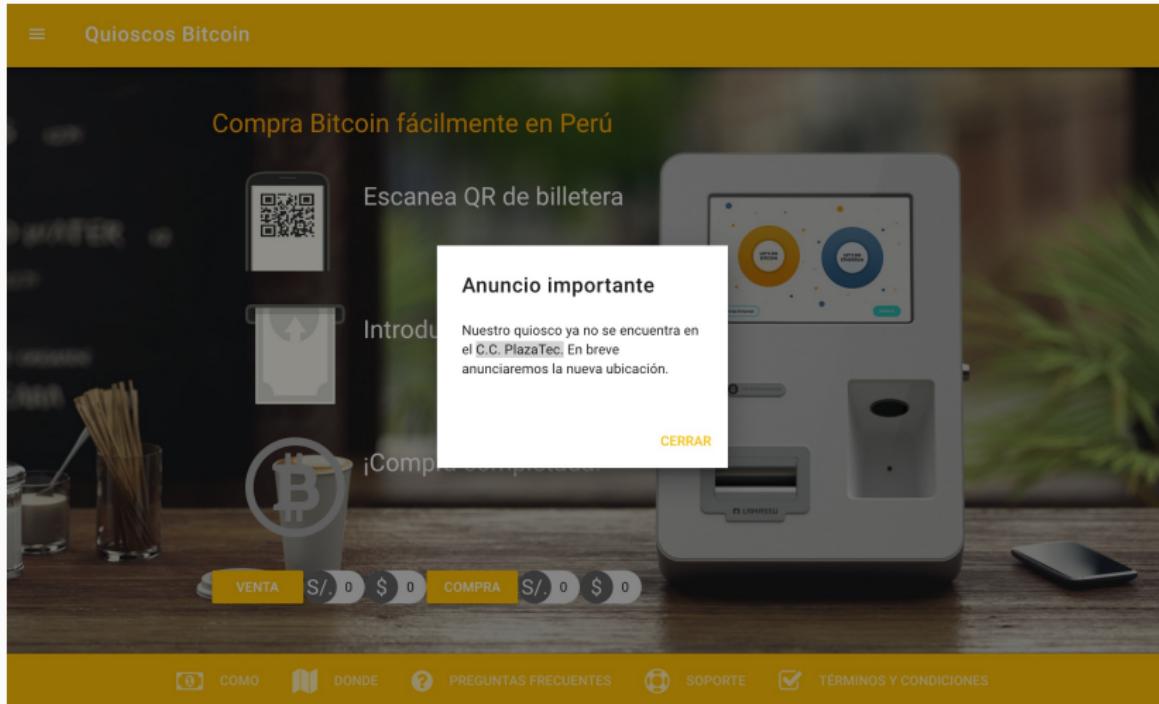
- Xapo
- Bitinka
- Cambista
- Surbtc
- P2P en grupos de FB, e.g. Bitcoin Peru.
- Primer cajero Perú: <https://quiosco.quinpu.com/>

Requerimientos usuales:

- DNI
- Teléfono celular
- Fotografía

Según Gestión, se instalarán cajeros para comprar Bitcoin en los principales centros comerciales de Lima en 2018. [Leer artículo.](#)

# Bitcoin: Perú (Cont.)



Fuente: [quiosco.quinpu.com](http://quiosco.quinpu.com)

# Alt–Coins: Aspectos del Mercado

## Top 100 Cryptocurrencies By Market Capitalization

Cryptocurrencies	Exchanges	Watchlist	USD	Next 100	View All			
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	...
1	Bitcoin	\$109,260,743,771	\$6,324.33	\$4,089,389,093	17,276,262 BTC	-0.79%		...
2	Ethereum	\$21,312,332,716	\$208.83	\$1,484,019,988	102,056,119 ETH	-1.21%		...
3	XRP	\$12,857,458,462	\$0.322978	\$550,953,956	39,809,069,106 XRP *	0.71%		...
4	Bitcoin Cash	\$7,441,467,701	\$428.73	\$293,862,648	17,356,888 BCH	-2.82%		...
5	EOS	\$4,569,622,734	\$5.04	\$550,042,167	906,245,118 EOS *	-0.77%		...
6	Stellar	\$3,859,248,619	\$0.205447	\$48,852,900	18,784,601,495 XLM *	-2.50%		...
7	Litecoin	\$3,108,155,459	\$53.26	\$249,012,341	58,359,906 LTC	-1.83%		...
8	Tether	\$2,736,361,195	\$0.992722	\$2,361,365,126	2,756,421,736 USDT *	-0.79%		...

Fuente: coinmarketcap.com

En general:

- 1 Criptomoneda educacional creada por la comunidad.
- 2 Programada en C++.
- 3 Con documentación para modificar el código fuente.
- 4 Con la misma estructura y parámetros que LiteCoin.

En particular<sup>1</sup>:

- 1 Total coins: 42 millones.
- 2 Block targets: 15 segundos.
- 3 Recompensa: 4 monedas por bloque generado.
- 4 Difficulty retargets: cada 0.35 das.

---

<sup>1</sup>Más detalles visitar el repositorio <https://github.com/bfroemel/smallchange>

## Definición 3.2 (Ethereum)

*Es una Blockchain pública de cómputo distribuido que permite crear códigos y desplegarlos. El lenguaje de programación es Solidity. El cómputo se realiza en los nodos (Ethereum Virtual Machine).*

## Definición 3.3 (Ether)

*Es la moneda criptográfica de la Blockchain de Ethereum.*

# Ethereum: Ether ≠ Bitcoin

## Ether vs. Bitcoin: aspectos técnicos

- Ether y Bitcoin son monedas criptográficas
- Ether es más veloz que Bitcoin.
- Ether utiliza Proof-of-Stake (PoS) en oposición a PoW.
- Ether está en java script y Bitcoin en C++.

## Ether vs. Bitcoin: aspectos comerciales

- Capitalizaciones de mercado:  $BTC \gg ETH > XRP$
- Ether tiene voceros con visibilidad, e.g. Vitalik Buterin.

## Definición 3.4 (Proof-of-Work)

Un Proof-of-Work (PoW) es un dato difícil de producir pero fácil de verificar y que satisface ciertos requerimientos. Bitcoin usa el PoW denominado Hashcash. El PoW es realizado por los mineros (miners).

## Definición 3.5 (Proof-of-Stake)

Un Proof-of-Stake es la riqueza del forjador (forger). La asignación del forger es pseudo-aleatoria, dependiendo de su nivel de riqueza. Un forjador que posee  $x\%$  de la moneda puede forjar hasta  $x\%$ .

Monedas que usan PoS: Ether BlackCoin, Lisk, Peercoin, Nxt Coin.

# Ethereum: Blockchain 2.0

Ethereum es la primera plataforma de su clase:

- Ethereum es una Blockchain para desarrolladores que pueden ejecutar sus scripts usando el poder computacional de los nodos.
- Script en Ethereum = Smart contract, e.g. Augur, Cryptokitties, etc.
- Ethereum marca el inicio de Blockchain 2.0.

Algunos ejemplos de contratos inteligentes son:

- Token nuevo: [ethereum.org/token](http://ethereum.org/token)
- Recaudación de fondos: [ethereum.org/crowdsale](http://ethereum.org/crowdsale)
- Organización democrática descentralizada: [ethereum.org/dao](http://ethereum.org/dao)
- Dapp nueva

# Ethereum: Solidity (Cont.)

Script para crear un token:

```
pragma solidity ^0.4.20;
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
    ) public {
        balanceOf[msg.sender] = initialSupply;           // Give the creator all initial tokens
    }
    /* Send coins */
    function transfer(address _to, uint256 _value) public returns (bool success) {
        require(balanceOf[msg.sender] >= _value);          // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                   // Subtract from the sender
        balanceOf[_to] += _value;                          // Add the same to the recipient
        return true;
    }
}
```

Fuente: [ethereum.org/token](https://ethereum.org/token)

## Ethereum: Solidity (Cont.)

Otros ejemplos de contratos inteligentes son:

- Recaudación de fondos: [ethereum.org/crowdsale](http://ethereum.org/crowdsale)
- Organización democrática descentralizada: [ethereum.org/dao](http://ethereum.org/dao)
- Dapp nueva

# Ethereum: Problemas Abiertos

Retos y controversias:

- Hack a un smart contract (The DAO): 60 MM USD robados.
- Ausencia de regulación vulnera a los inversionistas.

## Definición 3.6 (DAO)

*Descentralized Autonomous Organization (DAO) fue un fondo de venture capital en Ethereum.*

- En Junio de 2014 se realizó un ataque contra el DAO.
- 14% del Ether estaba en el DAO al momento del ataque, aproximadamente \$60M.
- El ataque logró trasladar un tercio de los fondos del DAO a una cuenta subsidiaria.
- En Julio de 2016 la comunidad de Ethereum decidió hacer un hard fork a la blockchain de Ethereum para restaurar los fondos.
- El resultado fue la división de Ethereum en dos blockchains, cada una con una moneda criptográfica diferente: Ethereum Classic (ETC) y Ethereum (ETH).

# Augur: Mercados de Predicción

The screenshot shows the Augur dapp interface with three prediction market cards:

- Market 1: Will FC Barcelona win against Real Madrid the next time they face on 28 October 2018?**
  - Open interest: 51.70% (down from 100%)
  - Volume: 84.4780 ETH
  - Fee: 1.0100 %
  - Expires: Oct 29, 2018 2:00 AM (UTC -5)
- Market 2: Who will win the 2018/19 English Premier League?**
  - Outcomes and percentages: Arsenal (4.50%), Chelsea (11.00%), Liverpool (20.00%)
  - Volume: 0.3924 ETH
  - Fee: 1.1211 %
  - Expires: May 13, 2019 2:00 AM (UTC -5)
- Market 3: Who will win the first 'El Clásico' match of 2018-2019?**
  - Outcomes and percentages: Barcelona (50.00%), Real Madrid (50.00%)

**Sidebar Navigation:**

- MARKETS: EOS ETHEREU..., SPORTS, ETHEREUM BL...
- CREATE: +
- PORTFOLIO: 📁
- REPORTING: 📈
- ACCOUNT: 🌐

Fuente: Augur dapp

# Augur: Precio

1 DAY 1 WEEK 1 MONTH 3 MONTH 1 YEAR ALL

REP/USD - Augur Market Price

MARKETS 55



Fuente: coinmarketcap

## Definición 3.7 (Augur)

*Es un oráculo descentralizado y una plataforma para mercados de predicción construída en la Blockchain de Ethereum.*

- Un principio: Juicio de la multitud (JM). Augur considera que el juicio de la multitud es (en promedio) más acertado que el de cualquier experto en particular. Idea: googlear eventos futuros.
- Funcionalidad: se puede construir un JM sobre cualquier evento (político, deportivo, etc.), i.e. asignar probabilidades de ocurrencia a cualquier evento conociendo los odds en su mercado de apuestas.
- Muchos problemas. Es posible que un participante que cree un mercado de apuestas sobre el cual tiene información privilegiada, o en el que tiene control sobre el resultado del evento.

## Nota 3.1 (Odds decimales)

Para odds decimales  $x$ , la probabilidad implícita del evento  $p(x)$  puede ser calculada como  $p(x) = 1/x$ . Si los odds de un evento son 1.65, es claro que el pago por acierto es 0.65 y por desacuerdo 0. En consecuencia la probabilidad implícita de que este evento ocurra es  $p(1.65) = 0.606061$ .

Ejemplos de mercados de predicción para realizaciones del tipo Sí/No :

### Ejemplo 3.1 (Real State)

¿Decrecerá el precio del metro cuadrado construido en San Isidro el 01.01.2020 con respecto a su valor en 01.01.2019?

### Ejemplo 3.2 (Social Media)

¿Subirá el número de usuarios de snapchat en 31.12.2019 en 200% con respecto a su valor en 31.12.2018?

## Augur: Controversia

Augur es exitoso:

- REP (su token) aumentó de precio en 2000% durante el 2017.
- Fue una de la dapps más usadas en 2017 (puesto 14).

Controversia:

- Deadpool: ¿Será Donald Trump asesinado en 2018?
- Augur considera que: "From the next presidential election to the success of a company's product. Anything is fair game."
- Augur considera que: el mercado de sicariato antecede a la creación de Augur, y existe en algunos websites de la llamada dark web.

### Más Información:

- Página web: <https://www.augur.net>
- Introducción oficial:  
<https://www.youtube.com/watch?v=yegyih591Jo>
- TruthCoin (competidor): <http://www.truthcoin.info>
- Otros competidores: Gnosis, Stox.

# Cryptokitties: Criptcoleccionables

It takes humans 9 months to make a baby, but in the same time you made 1,000,000 CryptoKitties!

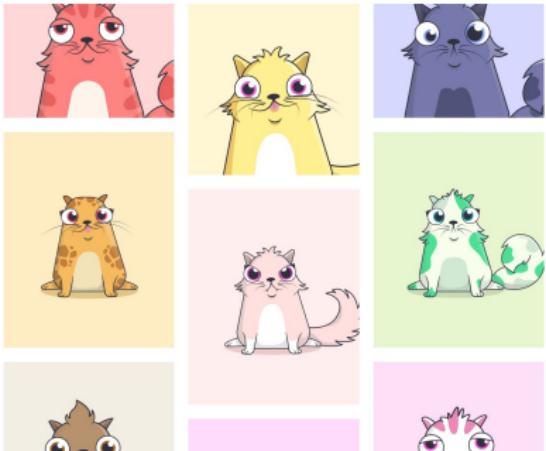
 CryptoKitties  Network Good

Catalogue  Search  FAQs  More 

**Collectible.  
Breedable.  
Adorable.**

Collect and breed digital cats.

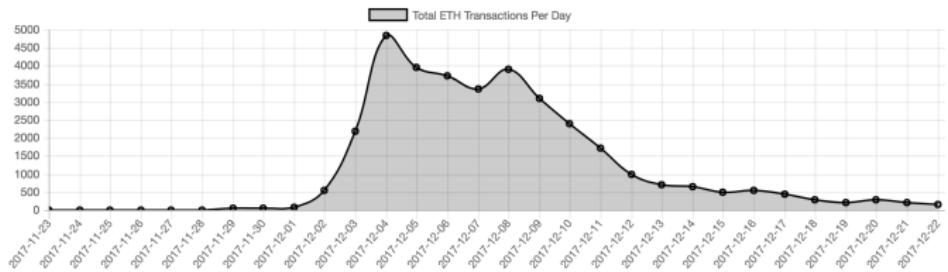




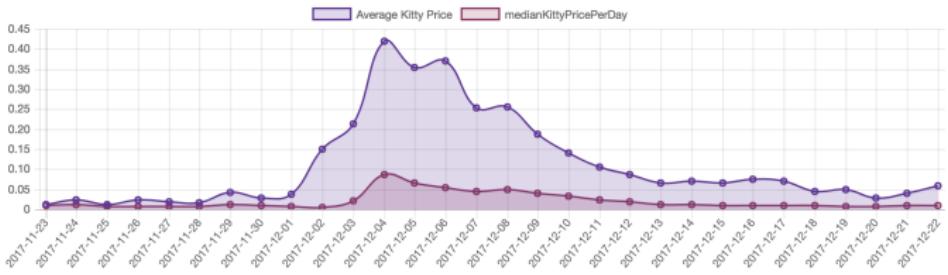
Fuente: [cryptokitties.co](https://cryptokitties.co)

# Cryptokitties: Precio

ETH Volume Per Day



Average Kitty Price by Day



Fuente: [cryptokitties.co](http://cryptokitties.co)

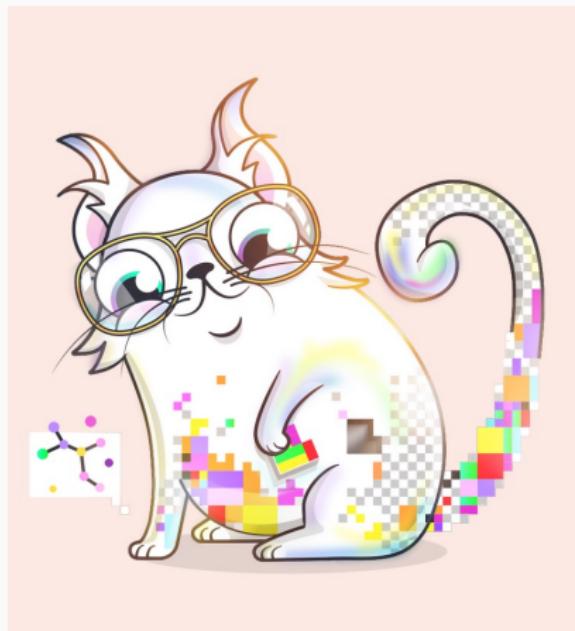
## Definición 3.8 (Cryptokitties)

*CryptoKitties es un juego virtual basado en blockchain desarrollado por Axiom Zen que permite a sus jugadores comprar, colecciónar, criar y vender diferentes tipos de gatos virtuales.*

- Los CKs son tokens no-fungibles, i.e. no son monedas criptográficas, que son puestos a disposición a una tasa de 1 cada 15 minutos.
- La propiedad de los CKs se registra en la Blockchain de Ethereum, i.e. no pueden ser replicados, transferidos o eliminados sin la autorización de su propietario.
- Cada CK posee una colección única de atributos (catributos), algunos de los cuales pueden ser transferidos a sus crías.

# Cryptokitties: Ejemplo

Mi Cryptokittie



## Cryptokitties: EtherScan

## En la Blockchain de Ethereum:

## Más Información:

- Página web: <https://www.cryptokitties.co>
- Tutorial para jugar: [https://www.youtube.com/watch?time\\_continue=119&v=dWUi8dkv5qU](https://www.youtube.com/watch?time_continue=119&v=dWUi8dkv5qU)
- En medios: <https://www.youtube.com/watch?v=jGfvkjzLrNw>
- Otros competidores: CryptoPunks, CryptoFighters, CryptoBots, CryptoPuppies.

Algunas de las críticas más recurrentes con respecto a Bitcoin (pero aplicables a cualquier otra moneda criptográfica) son las siguientes:

- Bitcoin está asociado a actividades ilícitas en la dark web.
- Bitcoin es una burbuja movida por una ideología libertaria fanática.
- Bitcoin es extremadamente volátil.

Y con respecto a los contratos inteligentes de Ethereum:

- Las ICOs han permitido la proliferación de smart Ponzis.
- La falta de regulación vulnera al inversionista.

Todas estas críticas son válidas en cierta medida.

# **Una moneda en C++**

---

# PHICoin: Una Criptomoneda en 5 Pasos



# Paso 1: Comunidad (ficción de 2 miembros)



1. Emulador  
de Linux para otro OS



2. Imagen  
de Ubuntu 14



3. Setup Usuarios  
2 máquinas virtuales



4. Clonar Moneda  
prototipo PHIcoin de GitHub



# Paso 1: Comunidad (ficción de 2 miembros)



## 1. Emulador

Descarga VMWare para el sistema operativo de tu computadora personal



Linux

<https://www.vmware.com/products/workstation-player.html>



Mac

<https://www.vmware.com/products/fusion.html>



Windows

<https://www.vmware.com/products/workstation-pro.html>

# Paso 1: Comunidad

[https://drive.google.com/open?id=12\\_OmgB6ZydiXc2UJJ-RZRXgWIHcRz3ak](https://drive.google.com/open?id=12_OmgB6ZydiXc2UJJ-RZRXgWIHcRz3ak)



## 2. Imagen

Descarga Ubuntu 14.

Una imagen con los requerimientos necesarios está disponible desde MEGA

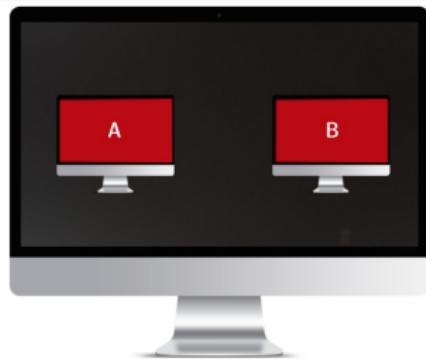


# Paso 1: Comunidad



## 3. Setup Usuarios

Descomprime el archivo. Crea dos copias de la carpeta (nómbralas „B“ y „A“).  
Inicia VMWare y desde allí inicia una sesión de B y otra de A.



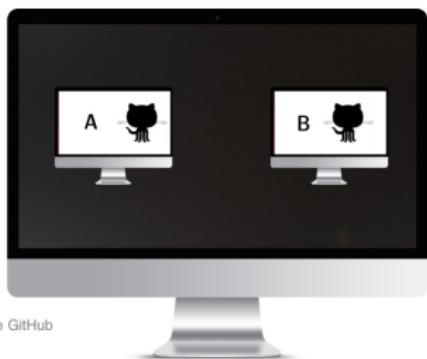
# Paso 1: Comunidad

```
> cd Documents  
> git clone https://github.com/PhiChain/PHICoin.git
```



## 4. Clonar Moneda

En A y B clona el repositorio de PHICoin desde GitHub



## Paso 2: Billetera (para cada miembro de la com.)



A      B

### Crea una billetera

```
> cd PHICoin/src  
> make -f makefile.unix  
> ./PHICoin
```

### Edita la billetera

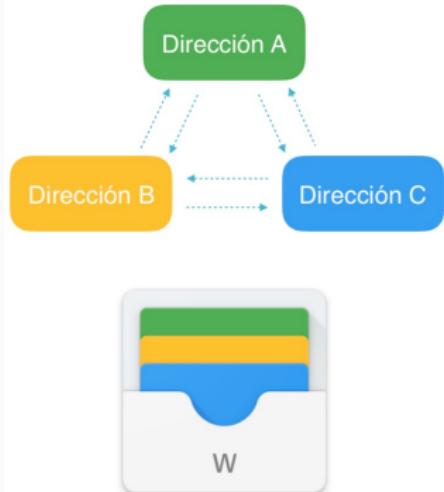
En A/B. Abre sublime. Edita. Guarda como „PHICoin.conf“

```
> rpcuser=<<usuario_unico>>  
> rpcpassword=<<contrasenna_unica>>  
> addnode=<<iP de B/A>>  
> addnode=174.138.59.134
```

## Paso 3: Minado (cada miembro es un minero)



## Paso 4: Transacciones (intra/inter billeteras)



Crea una cuenta y una dirección pública  
./PHICoin getnewaddress "tu\_nombre\_de\_Cuenta"

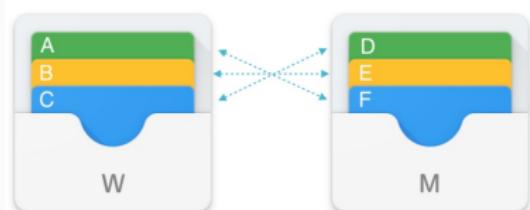


Visualiza tus cuentas y sus montos  
./PHICoin listaccounts



Transfiere a cuentas en la misma billetera  
./PHICoin move "desde\_cuenta" "hacia\_cuenta" "monto"

## Paso 4: Transacciones (intra/inter billeteras)



Transfiere a cuentas en diferentes billeteras

`./PHICoin sendtoaddress "dirección_billetera" "monto"`



Visualiza el estado de la transacción

`./PHICoin gettransaction "hash_de_transacción"`

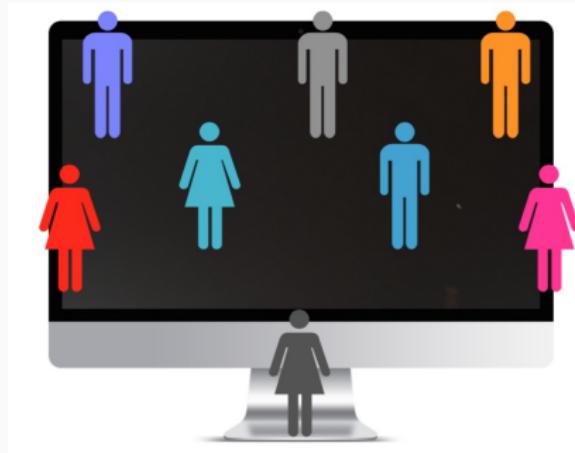
## Paso 5: Consultas (ver trans. en la red)

-  Visualiza información de los bloques minados  
`./PHICoin listsinceblock`
  
-  Visualiza las transacciones minadas en tu nodo  
`./PHICoin listtransactions`
  
-  Visualiza los bloques confirmados  
`./PHICoin listunspent`

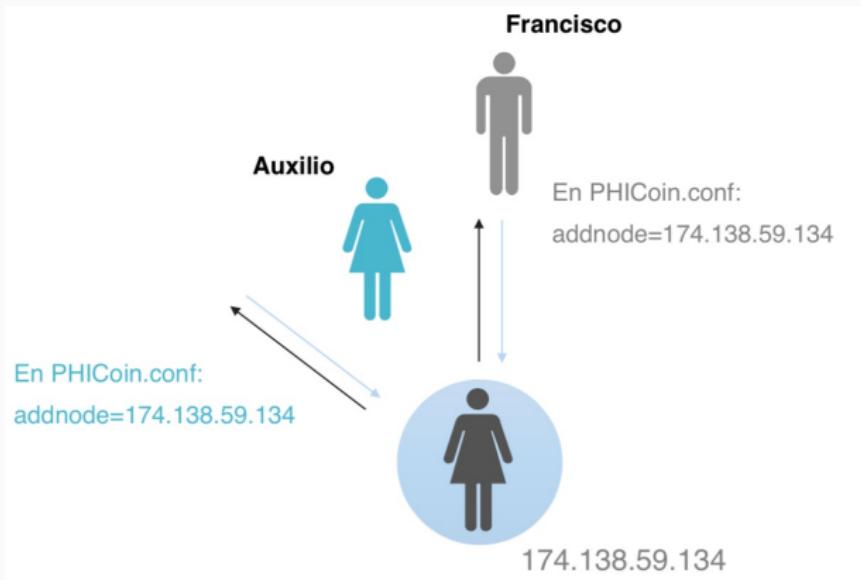


Blockchain

## Una Extensión: n miembros



## Una Extensión: n miembros



# Una Extensión: n miembros



# Evaluación 1

---

# Preguntas

Explique en sus propias palabras:

- 1** ¿En qué consiste el problema del gasto doble?
- 2** ¿Qué es una función hash y para qué sirve?
- 3** ¿Qué problemas resuelve la tecnología blockchain? (liste 2)
- 4** ¿Qué problemas puede crear la tecnología blockchain? (liste 2)
- 5** ¿Qué es un criptcoleccionable? (mencione un ejemplo)

# **Una Moneda en Solidity**

---

## **Blockchains Privadas**

---

## **Esquemas Ponzi y Pirámides**

---

## **Retos y Preguntas Abiertas**

---

## Evaluación 2

---

# Preguntas

Elija una de las siguientes opciones

- 1** Crear una moneda criptográfica en C++ siguiendo la sección 4.
- 2** Crear un contrato inteligente en Solidity y desplegarlo en la blockchain de prueba de Ethereum.