

Blockchain

Blockchain & Money



Casos reales, escándalos y conceptos clave
Curso 2024/2025



Francisco Hernando Gallego



fhernando@uva.es



Diego Martín de Andrés



diego.martin.andres@uva.es

Índice de contenidos




1. Estafas y esquemas Ponzi
2. Casos reales de estafa
3. Efecto Milei
4. Efecto Elon Musk
5. Qué pasó con FTX
6. Otros escándalos conocidos
7. ¿Blockchain o Base de Datos?


Índice de contenidos

- 8. ¿Cómo se crea una criptomoneda?
- 9. Firma electrónica y Blockchain
- 10. Cómo se minan bloques
- 11. ¿Cómo se ve una transacción en Blockchain?
- 12. Ejemplo: la caja fuerte
- 13. Conclusión y repaso final
- 14. CryptoZombies (con Solidity)



Grandes estafas y esquemas Ponzi

-  **Esquema Ponzi:** una estafa que promete ganancias altas y rápidas usando el dinero de personas nuevas para pagar a las anteriores.
-  Ejemplos de lo que prometen:
 - "Gana 10% al mes sin riesgo"
 - "Tu dinero trabaja por ti, sin que hagas nada"
-  Se disfrazan de inversiones reales:
 - Oro y metales preciosos
 - Criptomonedas falsas o poco conocidas
 - Apps de trading que no existen o no funcionan

-  Cómo evitan ser detectados:
 - Usan criptomonedas difíciles de rastrear, como Monero
 - Operan en plataformas sin regulación ni supervisión
 - Cuentan con redes de usuarios anónimos que reclutan más gente

Ejercicio:

¿Qué elementos comunes tienen estas estafas? Haz una lista de 3 señales de alerta que hayas visto o escuchado.

- Prometen ganancias rápidas que parecen demasiado buenas para ser verdad.
- No dan información clara ni transparente sobre cómo funciona la inversión.
- Piden que invites a más personas para poder ganar dinero, lo que es típico de un esquema Ponzi.

🕶 ¿Cómo intentan ocultarse en Blockchain?

Aunque las transacciones en blockchain son públicas, se puede ocultar el rastro:

1. Mezcladores (Mixers)

- Agrupan y mezclan muchas transacciones para dificultar el seguimiento.
- Ejemplo: Tornado Cash (prohibido en EE.UU.).

2. Criptomonedas privadas

- Como **Monero**, **Zcash** o **Dash**, que ocultan origen, destino y cantidad.
- Son preferidas en actividades que buscan anonimato total.

3. Cadenas puente (bridges)

- Permiten mover fondos entre distintas blockchains para dificultar el rastreo.

4. Fragmentación de transacciones

- Se divide una gran operación en muchas pequeñas (técnica conocida como "dusting").

Ejercicio:

¿Crees que debería ser posible ocultar tu identidad en blockchain? ¿Por qué sí o por qué no?

- **Sí**, cuando se trata de proteger privacidad en contextos legítimos (activismo, derechos humanos, censura).
- **No**, si se usa para lavar dinero, evadir impuestos o cometer fraudes.
- Idealmente, se necesita un equilibrio entre trazabilidad y privacidad.

Casos reales de estafa

- **OneCoin:** una criptomoneda falsa que estafó a miles de personas, robando unos 4.000 millones de dólares.
- **Bitconnect:** prometía beneficios fijos diarios, algo muy sospechoso porque el mercado cambia cada día.
- **Mt. Gox:** uno de los primeros grandes exchanges de Bitcoin, que perdió cerca de 850.000 bitcoins en un hackeo, dejando a muchos usuarios sin su dinero.
- **Terra/LUNA:** una stablecoin algorítmica que colapsó en 2022, causando grandes pérdidas y mostrando riesgos en criptomonedas que intentan mantener su valor con mecanismos complejos.

- Señales típicas de estafa:
 - Promesas vagas y poco claras
 - Rentabilidad garantizada sin riesgos
 - Falta de regulación o supervisión oficial
- Ejemplo sencillo: si alguien promete que siempre ganarás dinero, sin perder nunca, ¡cuidado!

Ejercicio:

Piensa en una oferta que hayas visto o escuchado que parecía demasiado buena para ser verdad. ¿Qué señales de alerta podrías identificar?

Respuesta:

- Promesas de ganancias seguras y sin riesgos.
- Falta de información clara sobre cómo se generan esas ganancias.
- Ausencia de regulación o supervisión oficial que garantice la seguridad.
- Ofertas que parecen muy atractivas pero no explican los detalles o riesgos.

Efecto Milei

- Javier Milei es un político argentino que quiere reducir el tamaño del Estado.
- Muchas personas en Argentina usan criptomonedas para:
 - Proteger su dinero de la inflación alta
 - Evitar el sistema bancario tradicional, que a veces falla o cobra mucho
- ⚠ Riesgos: sin control ni regulación, pueden aparecer estafas o fraudes.
- Ejemplo: alguien compra criptomonedas para ahorrar, pero si no sabe bien cómo funcionan, puede perderlo todo.

Ejercicio:

¿Qué ventajas y riesgos ves en usar criptomonedas para proteger tu dinero?

Respuesta:

Ventajas:

- Protegen contra la inflación cuando la moneda local pierde valor.
- Permiten evitar bancos tradicionales que pueden fallar o cobrar comisiones altas.

Riesgos:

- Falta de regulación puede facilitar estafas.
- Si no se entiende bien cómo funcionan, se puede perder todo el dinero.
- La volatilidad puede causar grandes pérdidas.



Efecto Elon Musk

- Elon Musk, empresario famoso, influye mucho en el mercado con sus tweets.
- Cuando habla de Dogecoin o Bitcoin, el precio puede subir o bajar rápidamente.
- 🌐 Esto muestra que el mercado de criptomonedas es muy emocional, no solo lógico.
- 💡 Lecciones importantes:
 - No te dejes llevar solo por lo que dice alguien famoso
 - Investiga y piensa antes de invertir
- Ejemplo: un tweet puede hacer que mucha gente compre o venda en minutos.


Ejercicio:

¿Por qué crees que las emociones afectan tanto al mercado de criptomonedas? ¿Cómo puedes evitar tomar decisiones impulsivas?

Respuesta:

- Las emociones afectan porque muchas personas compran o venden rápido basándose en noticias o comentarios, sin analizar bien.
- Para evitar decisiones impulsivas, es importante investigar, informarse bien y no dejarse llevar solo por opiniones de famosos.
- Pensar a largo plazo y tener un plan de inversión ayuda a controlar emociones.

¿Qué pasó con FTX?

- FTX era uno de los exchanges (plataformas para comprar y vender criptomonedas) más grandes y confiables.
- Usaban el dinero de sus clientes para hacer apuestas y especulaciones arriesgadas.
- En 2022, la empresa colapsó y muchos clientes perdieron sus ahorros.
-  Problemas: mala gestión, falta de transparencia y control.
- Ejemplo: como si alguien guardara tu dinero y lo usara para jugar a la ruleta sin avisarte.

Ejercicio:

¿Qué preguntas harías antes de confiar tu dinero a una plataforma de criptomonedas?

Respuesta:

- ¿Está regulada y supervisada por alguna autoridad?
- ¿Cómo protege mi dinero y mis datos?
- ¿Qué transparencia tiene en sus operaciones y gestión?
- ¿Qué experiencia y reputación tiene la empresa?
- ¿Ofrece garantías o seguros para proteger mis fondos?

⚠️ Otros escándalos conocidos

- 🚬 Mt. Gox (2014)
 - Uno de los primeros grandes exchanges de Bitcoin
 - 🗝 Hackeo masivo → pérdida de **850.000 BTC**
 - ❌ Usuarios perdieron sus fondos
 - 📦 Provocó crisis y desconfianza global
- 💣 Terra/LUNA (2022)
 - Stablecoin algorítmica que prometía mantener valor estable
 - 🔁 Mecanismo fallido → colapso total
 - 📉 Miles de inversores perdieron sus ahorros
 - 📱 Ejemplo de lo peligroso que puede ser confiar en sistemas sin pruebas sólidas

Ejercicio:



¿Qué lecciones podemos aprender de estos escándalos para proteger nuestro dinero?

Respuesta:

- No confiar ciegamente en plataformas o criptomonedas sin investigar.
- Entender los riesgos y cómo funciona la tecnología detrás.
- Buscar empresas reguladas y con buena reputación.
- Diversificar inversiones para no perder todo en un solo lugar.
- Estar atento a señales de alerta y evitar promesas de ganancias garantizadas.

Mini reto: ¿Blockchain o Base de Datos?

 ¿Qué tecnología usarías en cada caso?

-  **Registro de estudiantes** →  Base de datos tradicional

| Se necesita privacidad y actualización frecuente.

-  **Donaciones públicas** →  Blockchain

| Transparencia y trazabilidad para todos.

-  **Chat entre amigos** →  Base de datos

| Información privada y dinámica.

-  **Voto electrónico** →  Blockchain

| Seguridad, integridad y auditoría pública.

- Blockchain es útil cuando necesitas confianza y nadie pueda borrar o cambiar datos sin permiso.
- Base de datos tradicional funciona para cosas simples y privadas.

Ejercicio:

Piensa en un ejemplo de tu vida diaria. ¿Usarías blockchain o base de datos?

- Para cosas que necesitan mucha seguridad y transparencia, como contratos o votos, usaría blockchain.
- Para información privada o que cambia mucho, como contactos o mensajes, usaría base de datos tradicional.
- La elección depende de si necesito que los datos sean inmutables y confiables para todos.


Ejercicio:

¿Qué te gustaría crear con un contrato inteligente? Piensa en algo sencillo que puedas programar.

Respuesta:

- Podría crear un contrato para dividir pagos entre amigos automáticamente.
- Un sistema para registrar votos en una encuesta pequeña.
- Un juego simple donde los usuarios puedan comprar y vender objetos digitales.
- Algo que me ayude a entender cómo funcionan las reglas automáticas en blockchain.

¿Cómo se crea una criptomoneda?

- Paso 1: Se define el nombre y símbolo (por ejemplo: `PEPE` , `SOL` , `FRANCOIN`)
- Paso 2: Se usa un lenguaje como Solidity o plataformas que lo hacen fácil (ej. Remix, CoinTool)
- Paso 3: Se sube a una red (Ethereum, Binance Smart Chain, etc.)
- Resultado: ¡Ya está en la red! Pero no significa que valga algo.
-  Muchas estafas crean "tokens" vacíos solo para atraer gente.

Ejemplo real:

Vitalik Buterin, creador de Ethereum, desarrolló una plataforma de código abierto que permite crear contratos inteligentes y nuevas criptomonedas.


Ejercicio:

Busca un generador de tokens online. ¿Cuáles son los pasos? ¿Te parece fácil crear uno?

Respuesta:

- Los pasos suelen ser elegir nombre y símbolo, configurar cantidad y características, y luego desplegar el token en una red.
- Muchas plataformas lo hacen con formularios sencillos y sin necesidad de programar mucho.
- Sí, crear un token básico es fácil, pero eso no garantiza que tenga valor o sea seguro.

Firma electrónica española y Blockchain

- En España puedes firmar documentos digitalmente con validez legal.
- Algunas firmas usan blockchain para:
 - Validar que el contenido no ha cambiado
 - Saber quién firmó y cuándo
- Esto es útil para documentos importantes como contratos o certificados.
-  Seguridad y confianza para documentos digitales.

Ejercicio:

¿Dónde crees que sería útil usar firma electrónica con blockchain? Da un ejemplo.

Respuesta:

- En contratos legales para asegurar que nadie cambie el documento después de firmado.
- En certificados académicos para validar autenticidad.
- En documentos oficiales del gobierno para evitar fraudes.
- En acuerdos entre empresas para tener prueba segura de la firma.

¿Cómo se minan bloques?

- Minar bloques es resolver un problema matemático difícil.
- Imagina que es como resolver un sudoku muy complicado:
 - i. El problema matemático es encontrar un número que, al combinarlo con la información del bloque, genere un resultado especial (hash) que cumpla ciertas reglas (como empezar con varios ceros).
 - ii. Los mineros prueban muchas combinaciones hasta encontrar la correcta.
 - iii. Cuando alguien encuentra la solución, la anuncia a todos.
 - iv. Los demás mineros verifican que la solución es válida y, si es así, se añade el bloque a la cadena.

- Quien resuelve primero gana una recompensa en criptomonedas.
- Esto asegura que los datos no se puedan cambiar sin que todos lo noten (inmutabilidad).
- Ejemplo: es como un concurso donde solo el primero en resolver gana.

Ejercicio:

¿Por qué crees que es importante que minar bloques sea difícil? ¿Qué pasaría si fuera muy fácil?

Respuesta:

- Es importante que sea difícil para evitar que alguien pueda controlar la cadena y cambiar datos.
- Si fuera muy fácil, cualquiera podría crear bloques falsos y manipular la información.
- La dificultad asegura que todos confíen en la seguridad y en la integridad de la blockchain.



¿Cómo se ve una transacción en Blockchain?

- Puedes consultar cualquier pago real en páginas como:
 - etherscan.io
 - blockchair.com
- ¿Qué se ve?
 - Dirección de quien envía y quien recibe
 - Fecha y cantidad
 - Estado: éxito o fallo
- Todo esto es **público y no se puede borrar**

Ejercicio:





Entra en etherscan.io y busca una transacción. ¿Qué puedes entender de lo que ves?

Respuesta:

- Puedo ver quién envió y quién recibió el dinero.
- La cantidad transferida y cuándo se hizo la transacción.
- Si la transacción fue exitosa o falló.
- Que toda esta información es pública y permanente, nadie puede borrarla.



Ilustración: caja fuerte

-  El bloque es como una caja fuerte digital que guarda información.
-  Se abre con una clave secreta, que se obtiene al minar.
-  Si alguien cambia algo, la caja fuerte se rompe y todos lo notan.
-  Todos los participantes guardan una copia para verificar que nadie mienta.

Ejercicio:

¿Cómo ayuda esta “caja fuerte” a que la información sea segura? Explica con tus palabras.

Respuesta:

- Porque sólo se puede abrir con la clave correcta, nadie puede cambiar lo que hay dentro sin que se note.
- Si alguien intenta modificar algo, todos los demás se dan cuenta porque sus copias no coinciden.
- Así se mantiene la información protegida y confiable para todos.

Conclusión

- Blockchain es una tecnología útil para proteger información y dinero digital.
- No es magia: hay que entenderla y usarla bien.
- Las estafas siguen existiendo, por eso es importante educarse.
- La mejor defensa es aprender y ser crítico con las ofertas.



Conceptos clave para recordar

- Blockchain es transparente y seguro, pero no infalible.
- Los fraudes existen incluso con tecnologías nuevas.
- Aprender y preguntar siempre antes de invertir.



CryptoZombies

- Aprende a programar en Solidity, el lenguaje de Ethereum, creando juegos con zombies.
- Es ideal para principiantes que quieren entender cómo funcionan los contratos inteligentes.
- 🎮 Puedes crear tus propios zombies y ver cómo funcionan los contratos.
- Página web: cryptozombies.io



CryptoZombies: Crea y ataca con tu zombi

- Aprender Solidity puede ser divertido: diseña zombis que luchan.
- Cada zombi tiene un ADN único y puede atacar a otros zombis.



Definimos el zombi:

```
pragma solidity ^0.8.0;

contract ZombieFactory {
    uint dnaDigits = 16;
    uint dnaModulus = 10 ** dnaDigits;

    struct Zombie {
        string name;
        uint dna;
        bool invisible;
    }

    Zombie[] public zombies;

    function _createZombie(string memory _name, uint _dna) internal {
        zombies.push(Zombie(_name, _dna, false));
    }

    function _generateRandomDna(string memory _str) private view returns (uint) {
        return uint(keccak256(abi.encodePacked(_str))) % dnaModulus;
    }

    function createRandomZombie(string memory _name) public {
        uint randDna = _generateRandomDna(_name);
        _createZombie(_name, randDna);
    }
}
```

Ejercicio final:

¿Qué has aprendido sobre blockchain y criptomonedas? Escribe 3 cosas importantes para recordar.

Respuesta:

- Que blockchain ayuda a proteger y asegurar la información de forma transparente.
- Que existen muchas estafas, por lo que hay que informarse bien antes de invertir.
- Que no todo lo que brilla es oro; es importante ser crítico y no dejarse llevar por promesas fáciles.