Criptodivisas – Impacto y futuro

Alejandro Fdez. Trigo

Tecnología, Informática y Sociedad – 20/21

Índice

- Un poco de historia
- Qué son y qué NO son criptomonedas
- Cómo funcionan, sus usos y la cadena de bloques
  - Bitcoin
  - Ethereum ←
- Minería
- Futuro
- Bibliografía y comentarios

Un poco de historia

B-Money ya introduce conceptos cómo PoW, pero no llega a implementarlos.

Creación de eCash — 1983

Creación de DigiCash — 1995

La NSA ya investiga los sistemas de pagos criptográficos* — 1996

Aparece el concepto de Criptomoneda — 1998

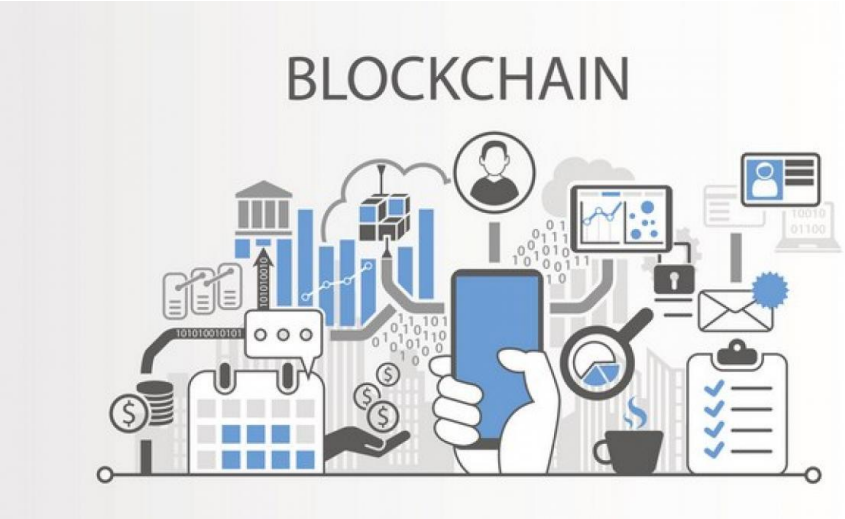
"Satoshi Nakamoto" crea la 1ª criptomoneda, el Bitcoin — 2009

* How to make a Mint: the Cryptography of Anonymous Electronic Cash – 1997 - https://archive.org/details/CryptographyOfAnonymousElectronicCash

Qué son y qué NO son criptomonedas

Para que un activo se considere como criptomoneda (criptodivisa) debe cumplir, al menos:

- Se fundamentan en un sistema DESCENTRALIZADO.
  - Este sistema emplea un algoritmo de consenso.
  - El sistema garantiza el anonimato de las transacciones (carácter criptográfico).
  - El sistema garantiza la consistencia de los datos.
  - El sistema establece una vía para crear nuevas unidades (“imprimir dinero”) y sus correspondientes límites, etc.



Qué son y qué NO son criptomonedas

Algunos ejemplos de criptomonedas:

Bitcoin

Ethereum

Litecoin

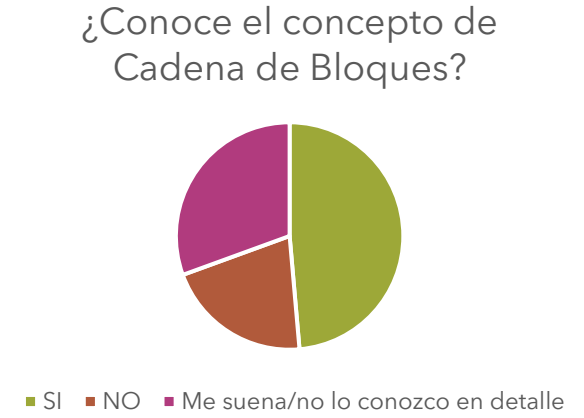
Dogecoin

Sin embargo, no lo son:

Petro venezolano

NFT's (Non-fungible token)

OneCoin
(Mayor esquema Ponzi de criptomonedas de la historia)



Cómo funcionan: Blockchain

Bases de datos centralizadas

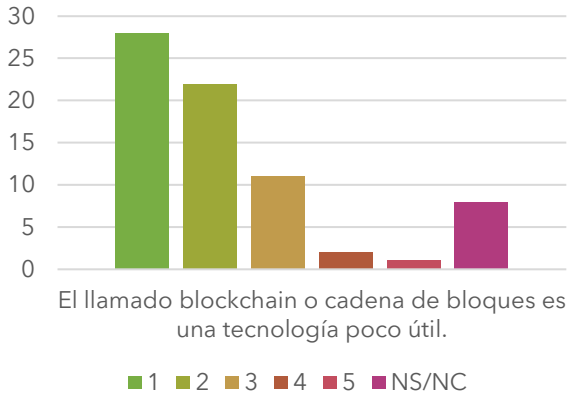
- Las de "toda la vida"
- Un centro, muchos usuarios
- La gestión depende completamente del "centro"

Bases de datos descentralizadas

- No son nuevas (¡P2P!)
- Muchos usuarios
- Los propios usuarios son los encargados de su gestión, ¿cómo?

Algoritmos de Consenso

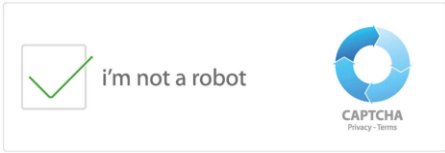
- Prueba de Trabajo (PoW)
- Prueba de Participación (PoS)



https://www.blockchain.com/btc/unconfirmed-transactions

Minería: Mantener el Blockchain

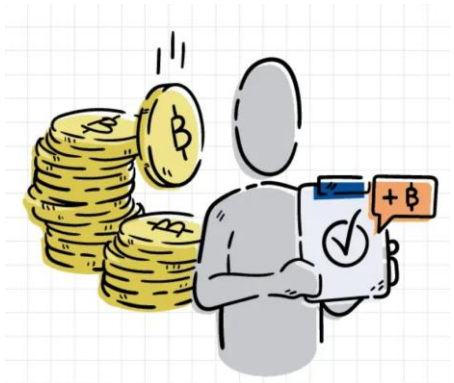
<<Todas las operaciones en una cadena de bloques distribuida requieren del "minado". Desde generar nuevas monedas hasta firmar contratos inteligentes, pasando por verificar transacciones.>>



Proof-of-Work (PoW) → el ejemplo más simple: el captcha.

La prueba de trabajo es la técnica de consenso más usada y más fácil de implementar; se realiza en cuatro fases:

1. Asignación de tareas
2. Resolución de tareas
3. Verificación de tareas
4. Confirmación

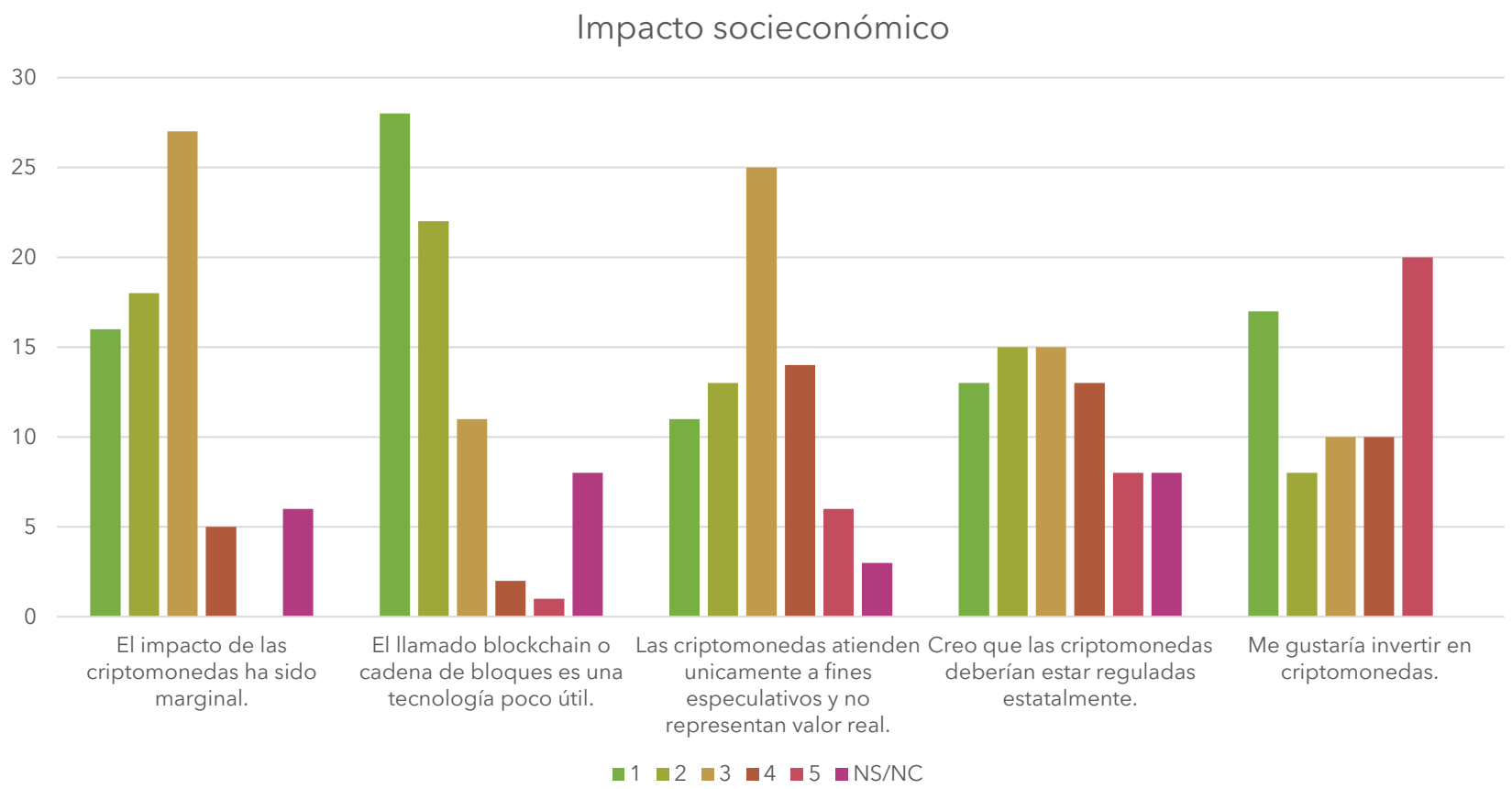


Proof-of-Stake (PoS) → creado para sustituir a la prueba de trabajo.

La decisión es 'aleatoria' pero el porcentaje aumenta para los 'validadores' que cumplen ciertos criterios establecidos. ¿Qué criterios? → A completa discreción del creador del algoritmo (con ciertas notas)*.

¿Qué pasa con los costes? → Eso es otro trabajo

Hasta ahora hemos visto un sistema DESCENTRALIZADO para el intercambio de valor real entre pares de forma anónima, pero hay más.



Futuro: Nos centramos en Ethereum

Se crea el concepto de ETH — 2013

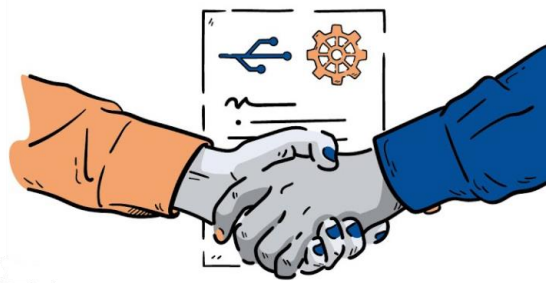
El ETH se hace realidad — 2015

Nace la Ethereum Alliance — 2017

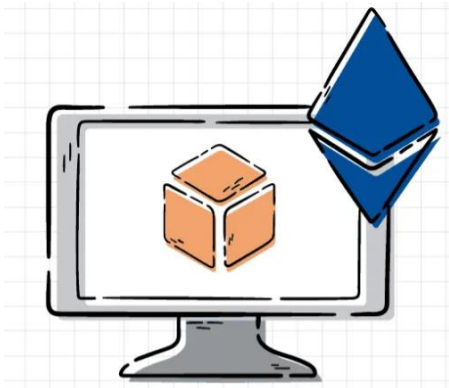
Ethereum 2.0
(https://ethereum.org/en/eth2/) — ¿Futuro?

Más allá de la simple emisión de monedas sustitutas del sistema "fíat", las cadenas de bloques más complejas pueden proporcionar características mucho mayores:

DApps



Smart Contracts



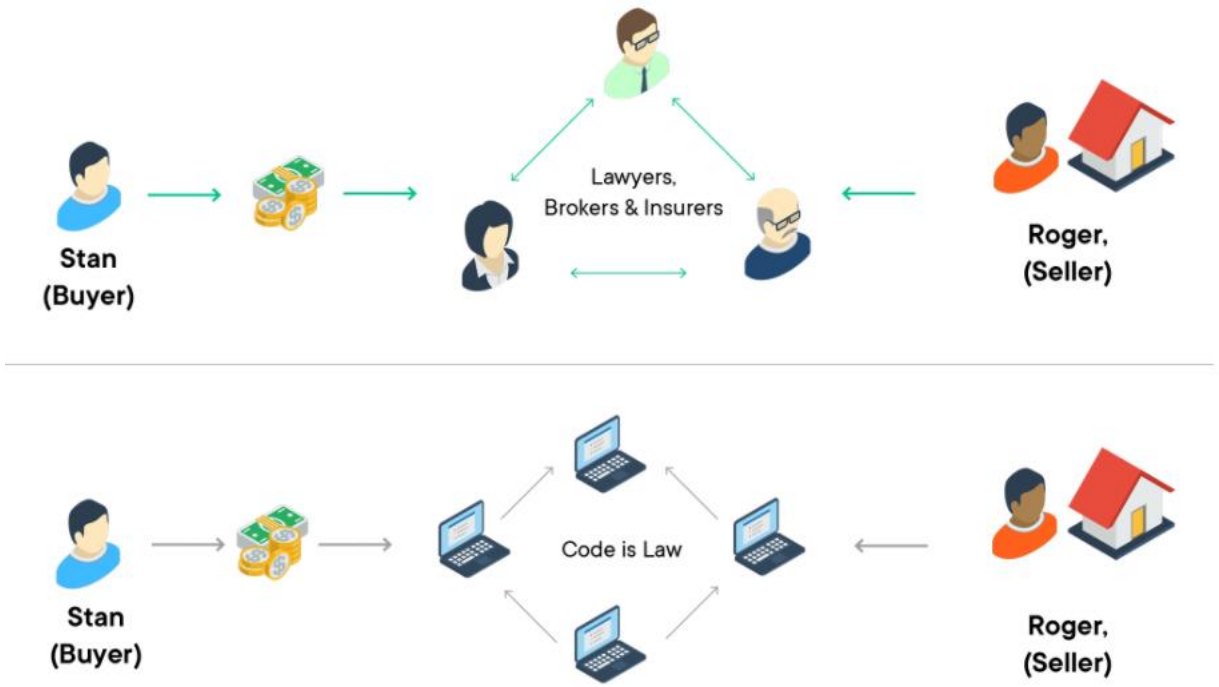
ETH Virtual Machine (EVM)

https://github.com/ethereum

Contratos Inteligentes

Hasta ahora las transacciones requerían de un intermediario, pero ¿y los contratos?

Los contratos inteligentes pueden entenderse cómo pagos programados, pero a diferencia de un servicio privativo (ej: Paypal), son transparentes.



Contratos inteligentes: Ejemplos

Sistemas de ‘trading’ automatizados

‘Smart property’ o registro de propiedades

Automatización de nóminas y/o pagos recurrentes

Otros

Registro de propiedad intelectual

DApps

Probablemente ya conozcas alguna DApp para descargar películas con dudosa legalidad (BitTorrent, uTorrent, etc) aunque la creación de Ethereum dio pie a muchas más alternativas.

Tipos

DApps tipo I (disponen su propia red)

DApps tipo II (emplean una blockchain, en nuestro ejemplo, la de Ethereum)

https://www.golem.network/

https://www.cryptokitties.co/

DApps tipo III (emplean una moneda generada por la blockchain (DApp tipo II) que usan)

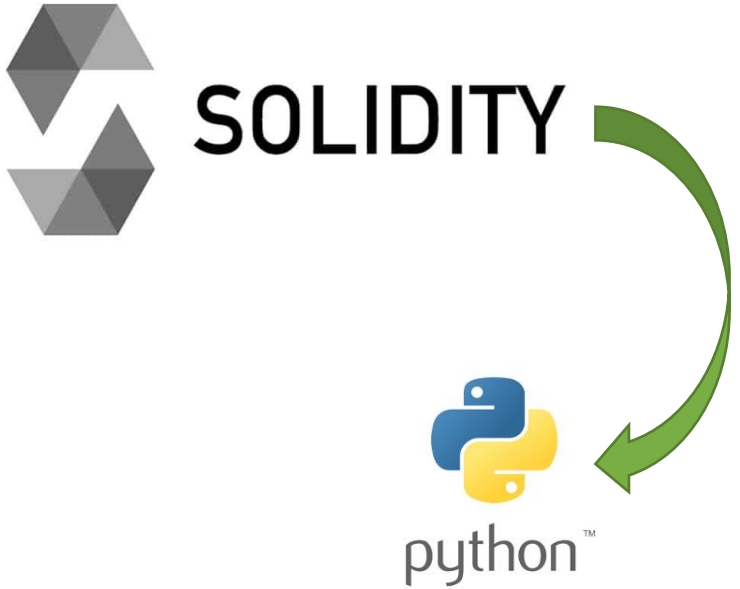
https://safenetwork.org/

https://ethereum.org/es/dapps/

EVM: Del papel al código

La Ethereum Virtual Machine o EVM es una máquina virtual dispuesta para ejecutar instrucciones de alto nivel sobre la red de bloques de Ethereum. Permite a 'cualquiera' crear contratos inteligentes para la blockchain.

```
pragma solidity 0.5.1;

contract MyContract {

    uint256 public peopleCount = 0;
    mapping(uint => Person) public people;

    struct Person {

        uint _id;
        string _firstName;
        string _lastName;

    }

    function addPerson(String memory _firstName, string memory _lastName) public {

        peopleCount += 1;
        people[peopleCount] = Person(peopleCount, _firstName, _lastName);

    }

    ......

}
```



https://solidity-es.readthedocs.io/es/latest/index.html

Problemas

- Falta de legislación y/o reconocimiento
- ¿Consumo? (otro trabajo que no abordaremos aquí)
- Falta de formación:
  - Estafas
  - ¿Otros?

Problemas: legislación/reconocimiento

Made for minds.

Búsqueda ACTUALIDAD

ACTUALIDAD MULTIMEDIA TV APRENDER ALEMÁN

AMÉRICA LATINA CORONAVIRUS POLÍTICA ECONOMÍA CULTURA CIENCIA Y ECOLOGÍA ALEMANIA HOY

ACTUALIDAD / ECONOMÍA

ECONOMÍA

España flirtea con el dinero virtual

España despunta en la tecnología de blockchain. Incluso los tradicionales grandes almacenes El Corte Inglés han registrado su propio nombre de moneda virtual: Bitcor.

Fecha 20.05.2021

Autor Claudia Stefanie Müller

Temas España, Bitcoin, Criptomoneda

Palabras clave Bitcoin, blockchain, Bitcor, El Corte Ingles, Elio, criptomoneda, España

Consultas y observaciones

EL PAÍS

MERCADOS MIS FINANZAS VIVIENDA FORMACIÓN MIS DERECHOS NEGOCIOS CINCO DÍAS RETINA ÚLTIMAS

Te quedan 9 artículos gratis este mes

TESLA MOTORS >

Tesla invierte 1.250 millones en bitcoins y aceptará pagos en la criptodivisa

El anuncio de la firma de Elon Musk dispara el precio de la moneda hasta máximos históricos, por encima de 44.000 dólares

China prohíbe a los bancos que operen con criptomonedas y el Bitcoin se hunde por debajo de los 40.000 USD

POR **Marta Gascón** NOTICIA 19.05.2021 - 11:46H

- La criptomoneda más popular ha caído este miércoles un 10%, llegando a los 38.973 USD, y ha arrastrado con ella al resto de divisas digitales.
- Elon Musk la sigue liando con Bitcoin: un tuit sugiere una venta masiva de Tesla de la criptomoneda y cae un 10%.

elEconomista.es

Mercados y Cotizaciones Ibex 35 M.Continuo ESG Empresas Economía Vivienda Status Opinión Más leídas Últimas

El bitcoin se desploma tras anunciar Musk que Tesla ya no acepta pagos con la criptomoneda

* *La decisión de la empresa se argumenta en razones medioambientales*
* *La criptodivisa cayó de los casi 55.000 dólares a 46.000 inmediatamente*
* *Ahora el bitcoin se acerca a los 51.000 dólares y recupera parte del terreno*

Home > Regulación

Zona Franca de Dubái permitirá el uso de bitcoin a turistas internacionales

Por Betssy Santistevan — 21 mayo, 2021 en Regulación 3 min de lectura

Problemas: Estafas

BENZINGA News Markets Ratings Ideas Fintech Investing Crypto Education Premium

QQQ 330.65 -1.82 -0.55% | DIA 341.01 + 0.51 + 0.15% | SPY 415.58 -0.30 -0.07% | TLT 136.79 + 0.44 + 0.32% | GLD 175.89 + 0.07 + 0.04%

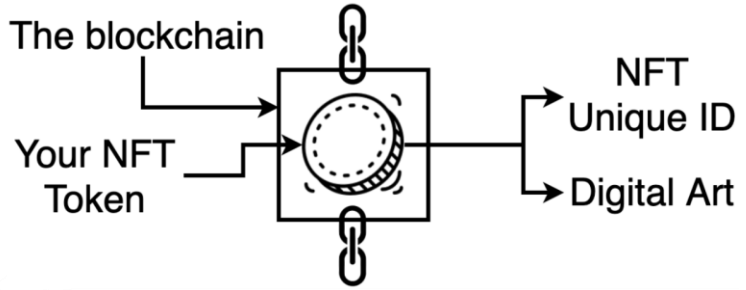
Tickers, Articles & Keywords

$32 Million Stolen As Crypto Project DeFi100 Pulls The Rug

by **Adrian Zmudzinski**
May 22, 2021 1:59 pm

¿Otros?

<<Los NFTs, Non-fungible tokens o tokens no fungibles NO son criptomonedas, pero si están basados en una cadena de bloques. Hay quien los denomina el 'futuro del arte'.>>



NFT: la historia detrás del famoso meme de la "niña desastre" que acaba de venderse por US$500.000

Redacción
BBC News Mundo

1 mayo 2021

Dave Roth, el padre de Zoë, tomó la foto en 2005.

Comenzó como una foto familiar, se volvió un meme y ahora se vendió por US$500.000.

Principales noticias

La enconada resistencia de Mindat, la pequeña ciudad que se enfrentó al ejército de Myanmar
4 horas

La condena al gobierno de Bielorrusia por desviar un avión "para detener a un periodista crítico"
2 horas

No te lo pierdas

Protestas en Colombia: "Es la primera vez que veo los estratos cinco y seis angustiados, y eso es bueno", Maurice Armitage, exalcalde de Cali
19 mayo 2021

Bibliografía y notas

Algunas fuentes:

- ''Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain: y no te atrevías a preguntar''
  - https://fama.us.es
- ''How To Make A Mint The Cryptography Of Anonymous Electronic Cash''
  - https://archive.org/details/CryptographyOfAnonymousElectronicCash
- ''NFTs, explained''
  - https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq
- ''Proof of Work VS Proof of Stake: Which One Is Better?''
  - https://www.bitdegree.org/crypto/tutorials/proof-of-work-vs-proof-of-stake#proof-of-stake-how-are-transactions-verified
- ''Bit2Me Academy''
  - https://academy.bit2me.com/
- Solidity documentation
  - https://solidity-es.readthedocs.io/es/latest/index.html

Sitios relevantes:

- https://ethereum.org/en/
- https://whattomine.com/
- https://www.blockchain.com/btc/unconfirmed-transactions (transacciones en tiempo real)

¿Alguna pregunta?