Ciclo Satoshi – 10º aniversario

economistas
Colegio de Valencia

Blockchain

Imagen: https://thenextweb.com/contributors/2017/08/13/blockchain-can-build-communities-completely-free-hierarchy/

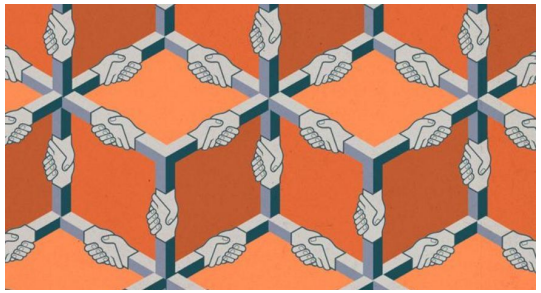
economistas
Colegio de Valencia

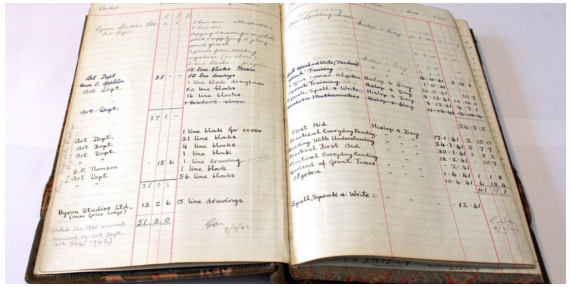
Qué es blockchain

Imagen: https://www.quora.com/What-is-blockchain-technology-1

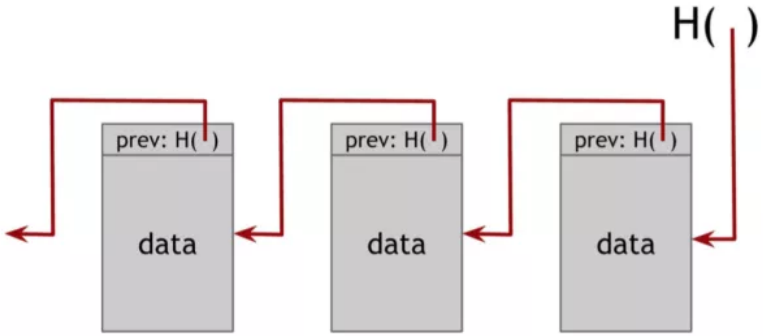
Blockchain

- Es una base de datos **distribuida** que contiene información sobre **transacciones y/o smart contracts**.





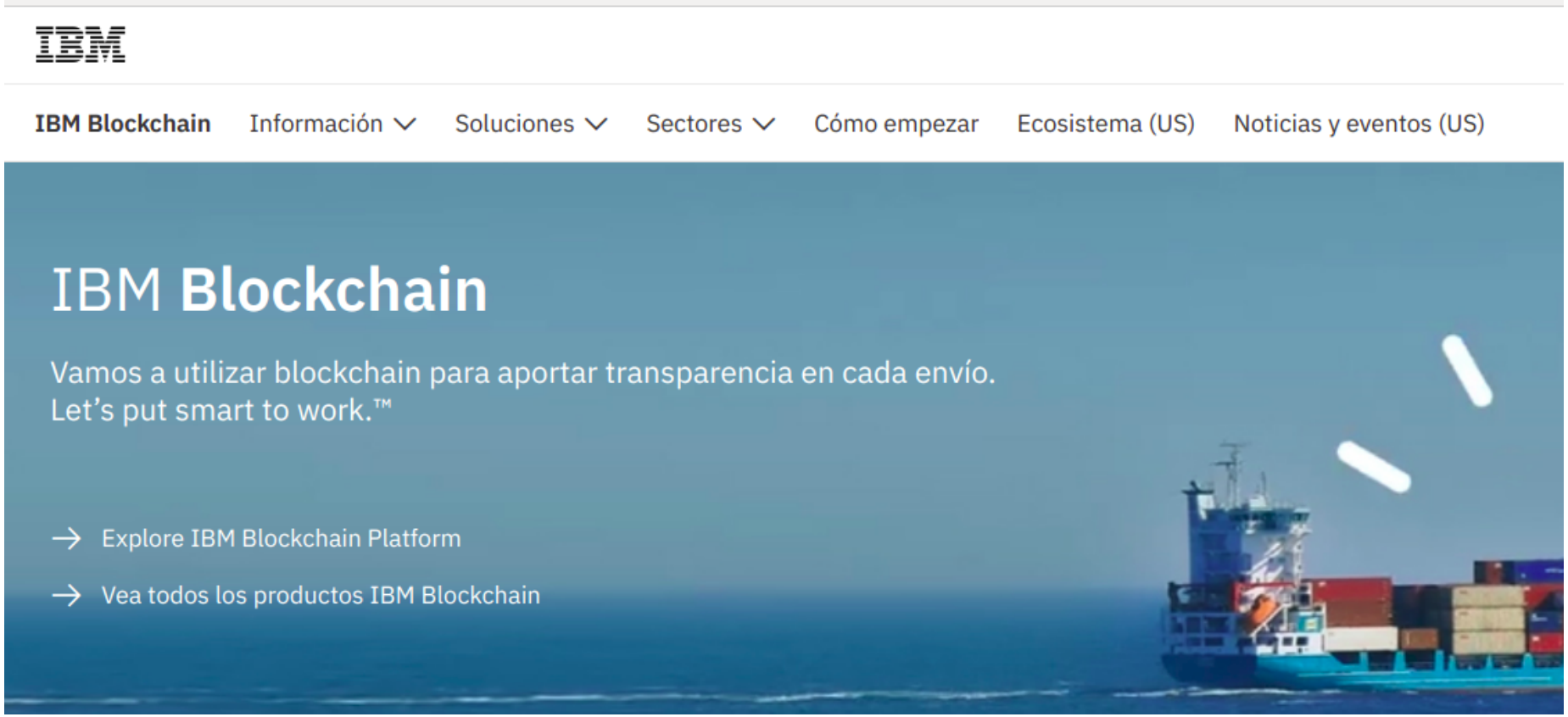
- La información se agrupa en bloques que están encadenados en base a algoritmos criptográficos.



Imágenes: https://www.criptonoticias.com/informacion/que-es-una-cadena-de-bloques-block-chain/
https://www.infotechnology.com/online/Que-es-blockchain-la-tecnologia-que-viene-a-revolucionar-las-finanzas-20160810-0001.htm

El caso de IBM

- La multinacional tecnológica IBM propone/vende en su web la utilización de la tecnología blockchain en varias líneas de negocio.



Fuente:
https://www.ibm.com/blockchain/es-es/?S_PKG=AW&cm_mmc=Search_Google-_-Blockchain_Blockchain-_-EP_ES-_-+Blockchain_Broad_AW&cm_mmca1=000024BV&cm_mmca2=10005803&cm_mmca7=1005545&cm_mmca8=kwd-305134168301&cm_mmca9=e29164d5-e488-4e96-a2c4-4bbc96435195&cm_mmca10=287989834281&cm_mmca11=b&mkwid=e29164d5-e488-4e96-a2c4-4bbc96435195%7C1394%7C6833&cvosrc=ppc.google.%2Bblockchain&cvo_campaign=000024BV&cvo_crid=287989834281&Matchtype=b

Un caso de uso

- Trazabilidad o seguimiento de los productos en el sistema alimentario.
- Veamos el video.

Red de seguridad alimentaria: IBM Food Trust™

Productores, distribuidores, minoristas y otros participantes mejoran la visibilidad y la responsabilidad en cada paso de la cadena de suministro de alimentos

Fuente: https://www.ibm.com/blockchain/es-es/use-cases/

economistas
Colegio de Valencia

Tipos de blockchain

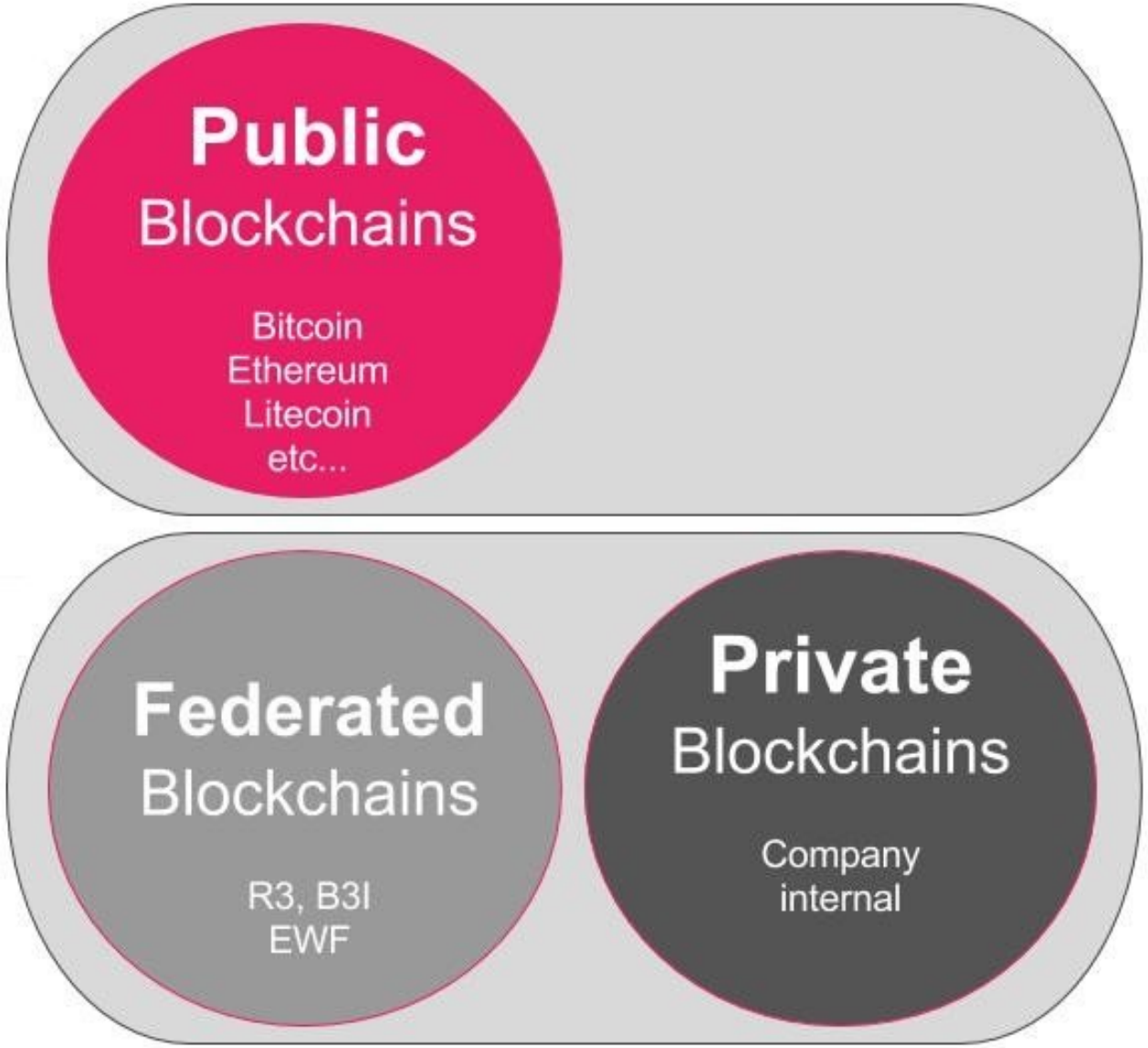
Imagen: https://blog.equinix.com/blog/2017/10/05/blockchain-a-new-type-of-internet/

economistas
Colegio de Valencia

Públicas – Federadas – Privadas

- Públicas
  - Cualquiera puede ver las transacciones y participar en el proceso de consenso.
- Federadas
  - No permiten que todos participen en el proceso de consenso. El acceso a la blockchain, sin embargo, puede ser público o restringido.
- Privadas
  - Pertenecen usualmente a una compañía. Solamente algunos miembros tienen permitido el acceso y llevar a cabo transacciones.

La posibilidad de acceso a la red está en dependencia de quién eres.



Fuente: https://www.bbntimes.com/en/technology/12-myths-about-blockchain-technology
https://blocktonite.com/2017/06/27/private-vs-public-and-permissioned-vs-permission-less/

economistas
Colegio de Valencia

Permisionadas – No permisionadas

- Permisionadas
  - Existe alguna entidad/entidades que deciden qué tipo de transacciones puede realizar un participante en la blockchain.
    - Ejemplo: https://chain.com

      Área de productos y servicios financieros.

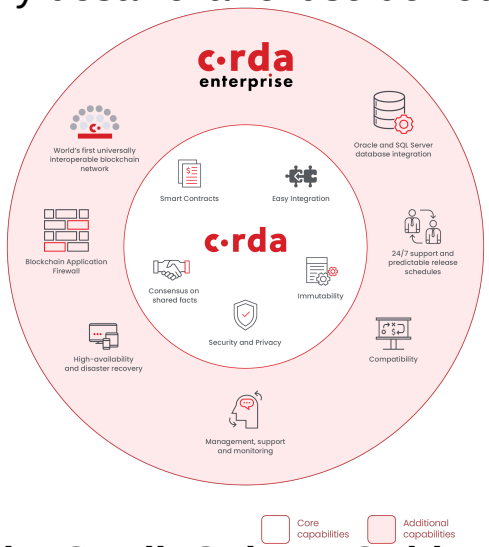
- No permisionadas
  - Las blockchain públicas son no permisionadas.

La posibilidad de acceso a la red está en dependencia de qué estás autorizado a hacer.

Fuente: https://blocktonite.com/2017/06/27/private-vs-public-and-permissioned-vs-permission-less/

R3: Blockchain tipo federada

- Lidera un consorcio de más de 200 empresas con la finalidad de investigar y desarrollar el uso del ledger distribuido en el sistema financiero y otras áreas de comercio.
  - Ha creado una DLT (Distributed Database Technology) llamada Corda con la finalidad de manejar transacciones complejas y restringir el acceso a los datos.

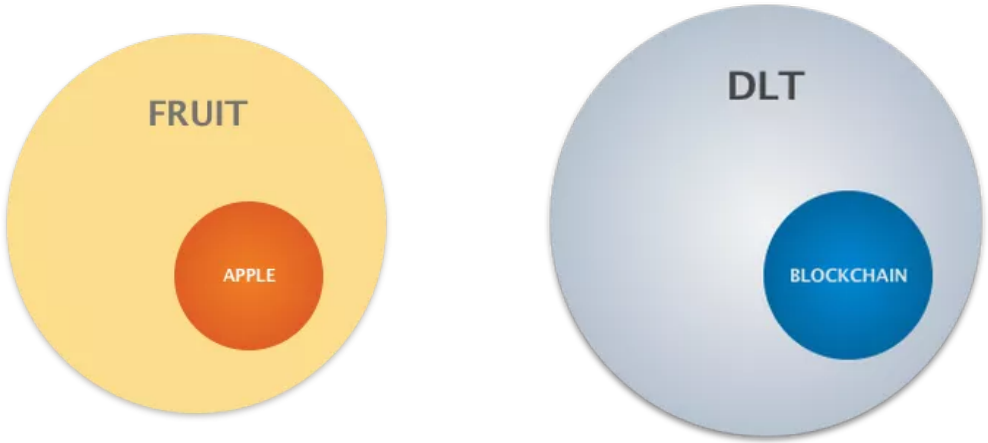


- Empezó en 2015 con: **Barclays**, **BBVA**, **Commonwealth Bank of Australia**, **Credit Suisse**, **Goldman Sachs**, **J.P. Morgan**, **Royal Bank of Scotland**, **State Street**, y **UBS**.
- Inmediatamente se unieron: **Bank of America**, **BNY Mellon**, **Citi**, **Commerzbank**, **Deutsche Bank**, **HSBC**, **Mitsubishi UFJ Financial Group**, **Morgan Stanley**, **National Australia Bank**, **Royal Bank of Canada**, **Skandinaviska Enskilda Banken**, **Société Générale**, y **Toronto-Dominion Bank**.

Fuente: https://en.wikipedia.org/wiki/R3_(company)

DLT vs blockchain

- Distributed Ledger Technology (DLT): base de datos de registros distribuida, es decir, no está almacenada o confirmada por una autoridad central.

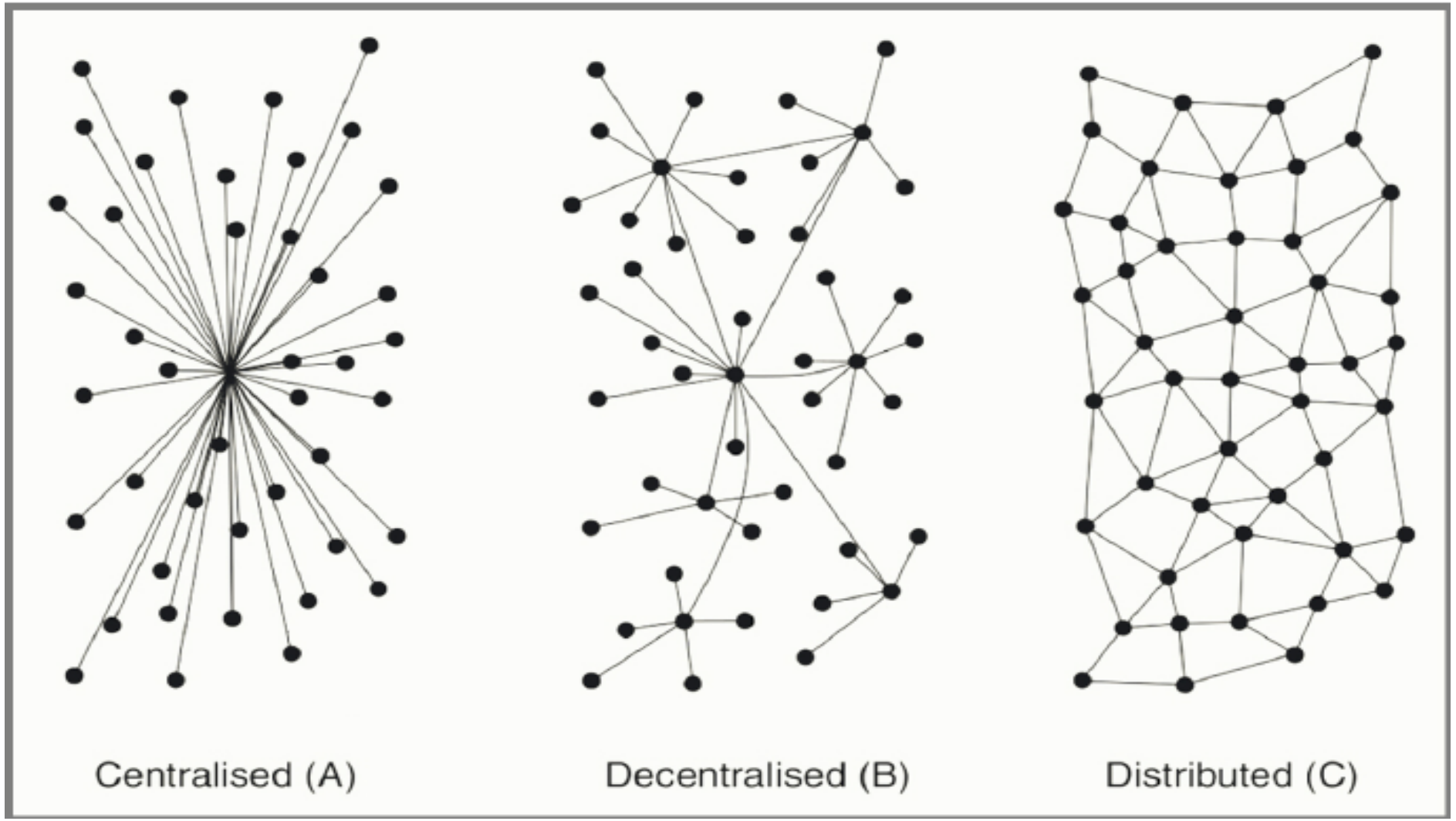


- Utilizar firmas criptográficas y almacenar registros en bloques son características de blockchain.

Fuente: https://thenextweb.com/hardfork/2018/07/27/distributed-ledger-technology-blockchain/
Imagen: https://www.mangoresearch.co/blockchain-vs-distributed-ledger-technology-dlt/

economistas
Colegio de Valencia

Centralizadas – Descentralizadas – Distribuidas



Fuente: https://www.researchgate.net/figure/Centralized-decentralized-and-distributed-network-models-by-Paul-Baran-1964-part-of-a_fig1_260480880

economistas
Colegio de Valencia

Técnicas de consenso

Imagen: https://twitter.com/educa_cons

Proof of Work

- La idea fue publicada por **Cynthia Dwork** y **Moni Naor** en 1993.
- La genialidad de Satoshi Nakamoto consistió en combinar ideas y conceptos existentes para crear un mecanismo de consenso completamente nuevo y fiable, no dependiente de personas.

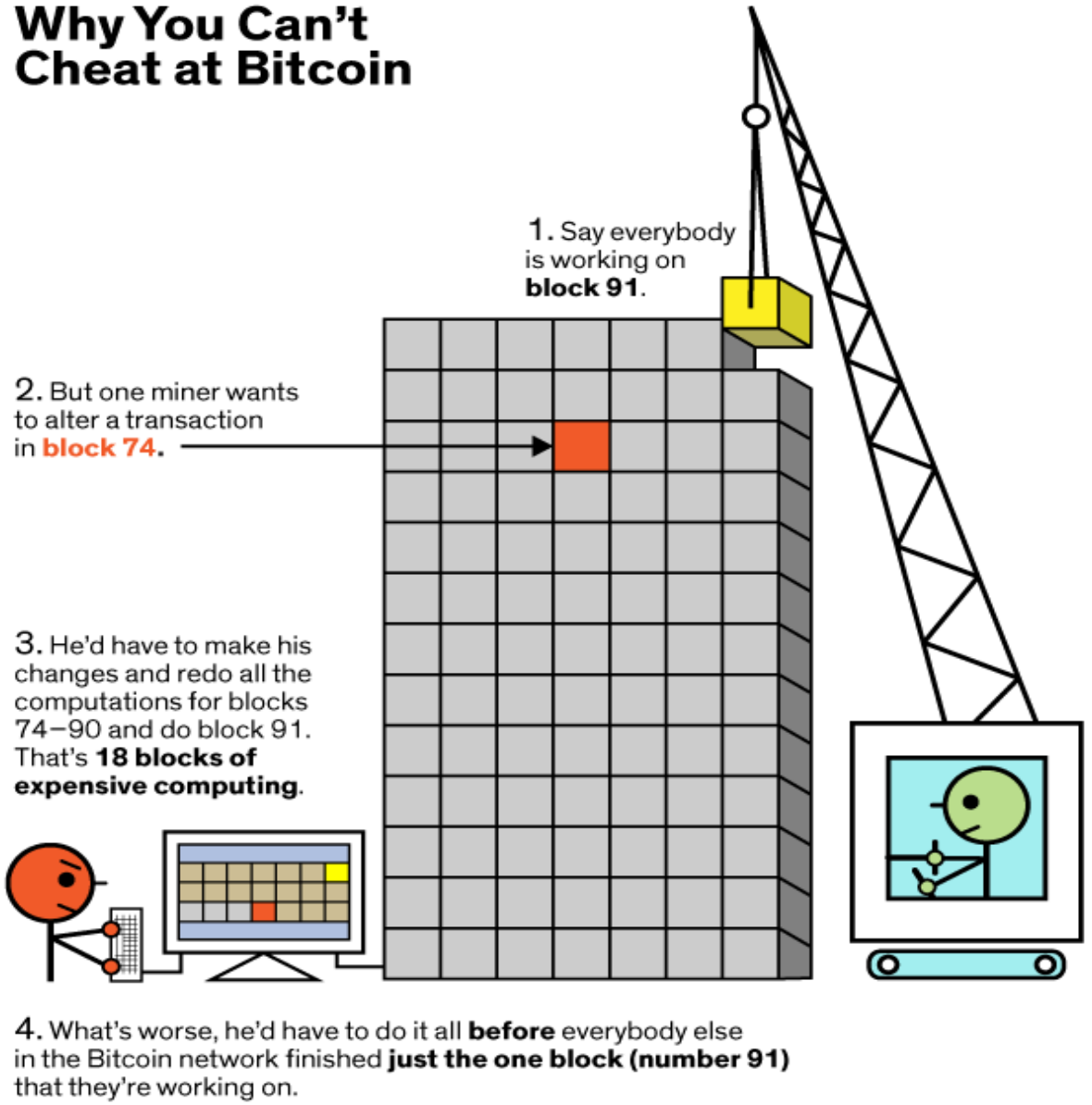
Fuentes: https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10
https://www.slideshare.net/DavidEvansUVa/the-blockchain

Proof of Work - II

- PoW requiere minado (potencia computacional), y el minado tiene un coste.

- Los mineros compiten, en el caso de bitcoin, por encontrar un nonce que produzca un resultado de hash del bloque con el número de ceros al principio que se les pide.
- La única forma de encontrar el nonce es mediante el método de “fuerza bruta”.

Ciclo Satoshi: Blockchain



Fuentes: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb

economistas
Colegio de Valencia

Proof of Stake

- El concepto de prueba de participación sostiene que una persona puede minar o validar las transacciones de un bloque de acuerdo a cuántas monedas posee.
- La primera criptomoneda en adoptar PoS fue Peercoin.
- El protocolo PoS asigna de forma aleatoria el derecho a validar un bloque entre los poseedores de mayor cantidad de unidades de moneda.

Fuentes: https://www.investopedia.com/terms/p/proof-stake-pos.asp
https://usethebitcoin.com/top-3-best-proof-of-stake-tokens-earn-cryptocurrency-by-hodling/

economistas
Colegio de Valencia

Proof of Stake - II

- Para que un nodo sea elegido “staker” o participante, su propietario debe haber depositado una cierta cantidad de monedas en una determinada wallet.
- El nodo creará nuevos bloques de forma proporcional a la cantidad de monedas que haya en su billetera. Por ejemplo, si se posee el 1% de las monedas, entonces se podrá "minar" el 1% de los nuevos bloques.

Fuentes: https://www.coinbureau.com/education/comprehensive-guide-pos-mining/

Ciclo Satoshi: Blockchain

- Proof of Work vs Proof of Stake

Fuentes: https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10

Ciclo Satoshi: Blockchain

Más Algoritmos de Consenso

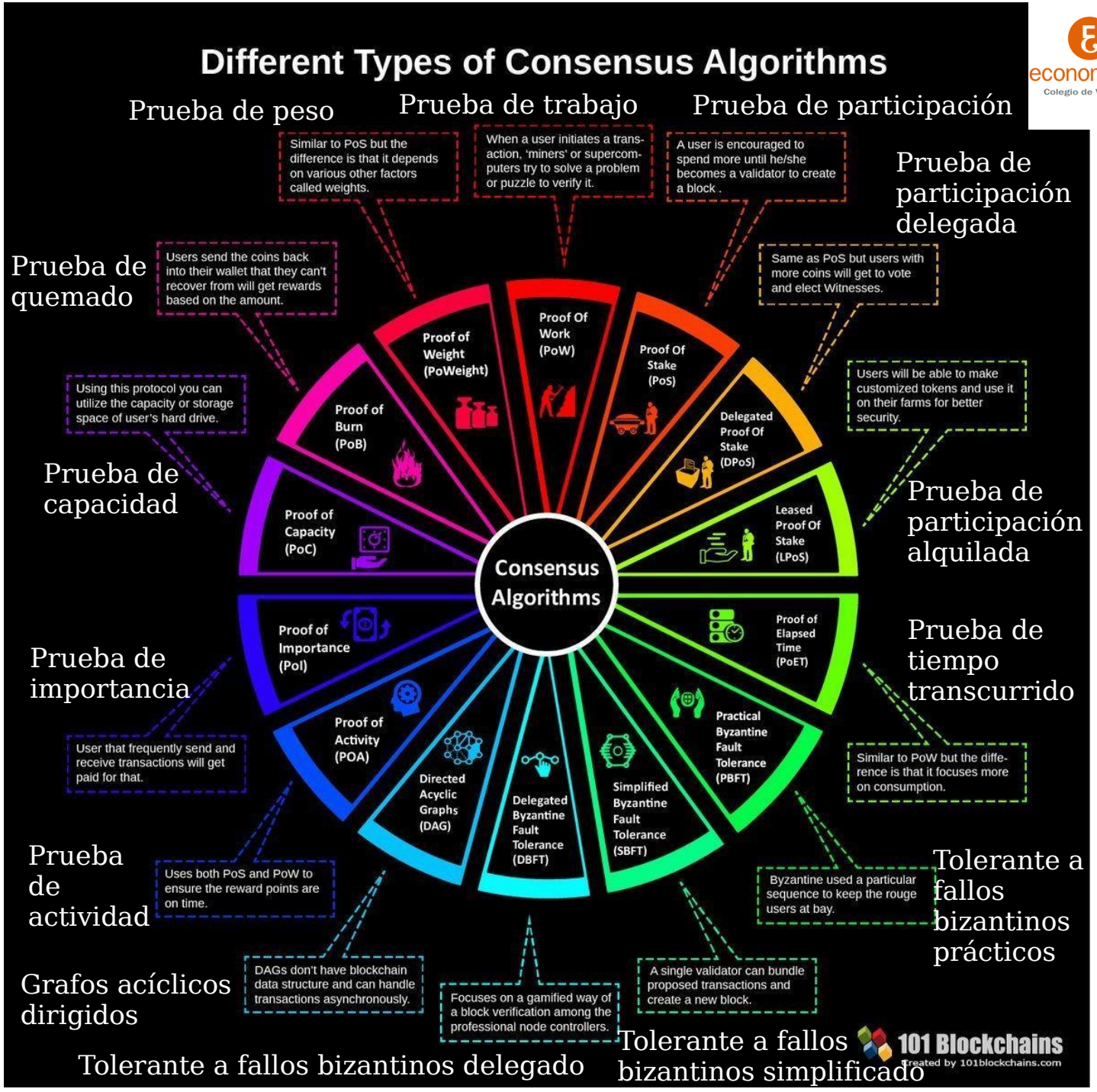


Imagen: https://image-store.slidesharecdn.com/a8feb5a3-884b-4397-8a77-e3709012174f-original.jpeg

economistas
Colegio de Valencia

Un par de ejemplos de blockchains

Imagen: https://www.mhlnews.com/global-supply-chain/lets-get-digital-supply-chains-are-going-get-smarter-2018

Hyperledger

HYPERLEDGER

economistas
Colegio de Valencia

- Su creación fue anunciada por la Fundación Linux en diciembre de 2015.
- Hyperledger es un proyecto “paraguas” de blockchains de código abierto para impulsar el desarrollo colaborativo de DLTs.
- Algunos miembros de la iniciativa: **ConsenSys**, **Digital Asset**, **R3**, **Onchain**, **Cisco**, **Fujitsu**, **Hitachi**, **IBM**, **Intel**, **Red Hat**, **VMware**, **Deutsche Börse Group**, **J.P. Morgan**, **State Street**, **SWIFT**, **Wells Fargo**, **SAP**, **Accenture**, …

Fuente: https://en.wikipedia.org/wiki/Hyperledger

Hyperledger II

HYPERLEDGER

- Gobernanza: según wikipedia, consiste en 20 miembros presididos por Blythe Masters, (CEO de Digital Asset), y 12 miembros del Comité de Dirección Técnica presididos por Christopher Ferris, CTO de Open Technology en IBM.

Blythe Masters

Christopher Ferris

Fuente: https://en.wikipedia.org/wiki/Hyperledger

Hyperledger Fabric

- Marco de trabajo de Hyperledger diseñado para la creación de chaincodes (smart contracts) en cualquier lenguaje de programación.
- Por defecto a la hora de implementar chaincodes se utiliza el lenguaje de programación de Google: Golang.
- Es posible elegir el tipo de consenso (pluggable consensus).

Fuente: https://medium.com/@_mtnieto/creando-una-red-privada-blockchain-con-hyperledger-fabric-2e1567167325

Alastria

... made in Spain ;-)

- “Red Blockchain/DLT semipública, independiente, permisionada y neutral, diseñada para ser conforme con la regulación existente, que permite a los asociados experimentar estas tecnologías en un entorno cooperativo”.
- “El Consorcio está abierto a cualquier organización que quiera disponer de una herramienta fundamental para desarrollar su propia estrategia Blockchain/DLT pensando en la distribución y organización de productos y servicios para el mercado español”.
- Veamos el video.

Fuentes: https://alastria.io/#1

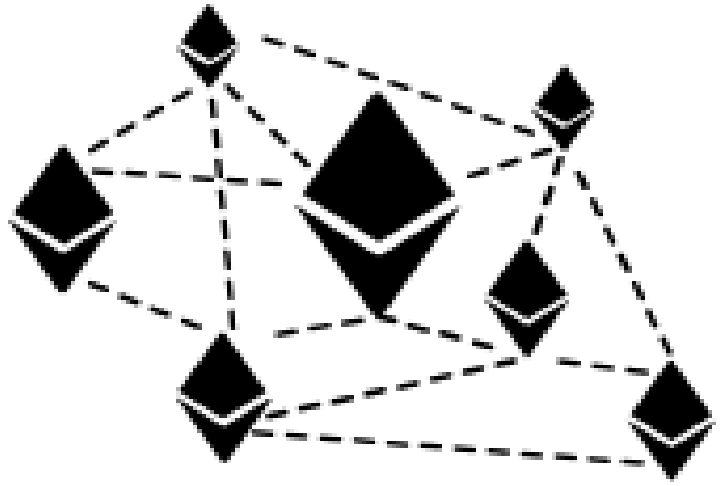
Consenso en Alastria

- “Alastria está construida sobre Quorum, la plataforma basada en Ethereum de JP Morgan”.
- “Las redes de Quorum procesan de docenas a cientos de transacciones por segundo, dependiendo de cómo se configuren la red y los contratos inteligentes”.
- “En lugar de proof of work (minería), Quorum utiliza los algoritmos de consenso QuorumChain, RAFT o Istanbul BFT basados en el voto. En el caso de Alastria, se está trabajando sobre Istanbul”.
- Nodos Validadores: “ejecutan el protocolo de consenso Quorum para validar las nuevas transacciones de Alastria. Cada "escritura" al libro mayor de Alastria se produce por un nodo de validación”.
- Nodos Aplicación: “serán necesarios a medida que la red se desarrolle, para distribuir la carga de lectura sobre el blockchain, garantizando la privacidad y confidencialidad de la información”.

Fuentes: https://alastria.io/en_que_se_basa

economistas
Colegio de Valencia

La blockchain Ethereum



Blockchain Ethereum

- Descrito inicialmente en un “white paper” por Vitalik Buterin en 2013, el proyecto Ethereum fue lanzado a través de una preventa de ether en agosto de 2014.
- La finalidad inicial era poder construir aplicaciones descentralizadas.
- El mecanismo de consenso es proof of work y tratan de evolucionar a proof of stake utilizando el protocolo Casper.

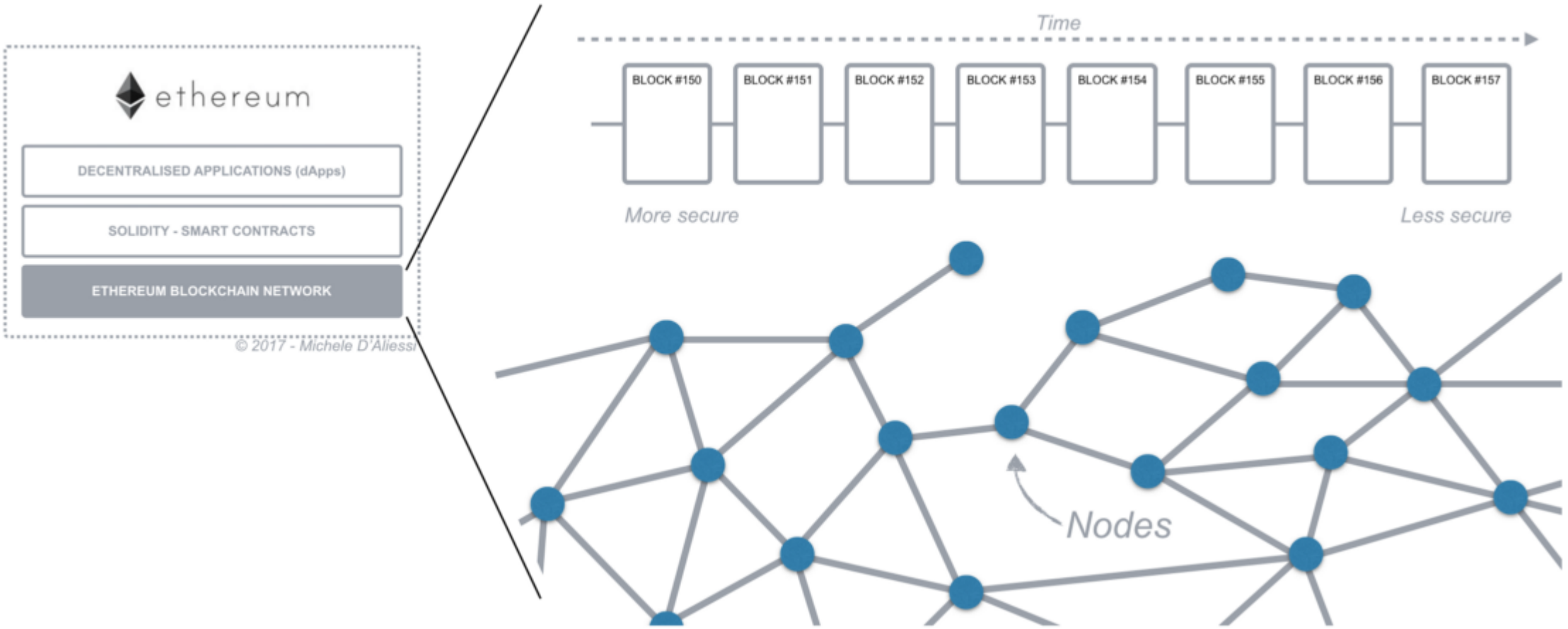
Fuentes: https://www.ethereum.org/
https://en.wikipedia.org/wiki/Ethereum

Ethereum blockchain

- El protocolo PoW en Ethereum se llama Ethash y funciona de manera ligeramente diferente al de Bitcoin, lo que permite que se pueda utilizar hardware común para la minería, en lugar de las ASICs (application-specific integrated circuit).
- La red Ethereum es pública y no permisionada.
- El token Ethereum se llama ether - ETH.

Fuentes: https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/

Red y bloques en Ethereum



Fuentes: https://medium.com/@micheledaliessi/how-does-ethereum-work-8244b6f55297

economistas
Colegio de Valencia

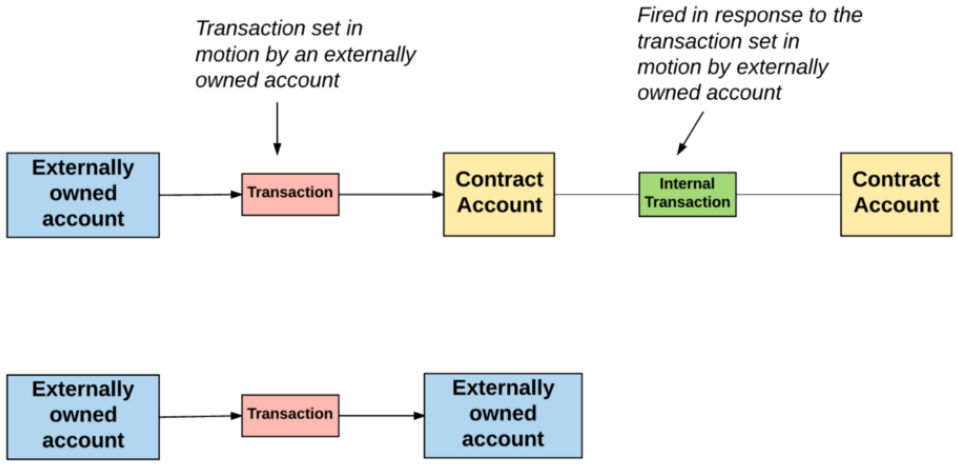
Red y bloques en Ethereum II

- La capa de hardware de Ethereum es una red de ordenadores peer to peer que computan las transacciones y las mantienen en orden en un libro mayor compartido.
- Esto les permite construir una base de datos distribuida que puede mantener un registro de todas las transacciones que tienen lugar.
- Cada ordenador en la red se llama "nodo".

Fuentes: https://medium.com/@micheledaliessi/how-does-ethereum-work-8244b6f55297

Cuentas en Ethereum

- Cuentas de contrato, que están controladas por su código de contrato y tienen un código asociado a ellas.



- Cuentas de propiedad externa, que están controladas por claves privadas y no tienen ningún código asociado a ellas.

Fuentes: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369

economistas
Colegio de Valencia

Qué es el Gas en Ethereum

- Es una medida de esfuerzo computacional.
- Se trata del coste que tiene una operación en Ethereum al realizar una transacción o al ejecutar un smart contract.
- Por ejemplo, calcular un hash cuesta 30 gas.
- Desglose de operaciones y costos de gas en yellow paper: http://gavwood.com/Paper.pdf
- 1 ether = 10^18 wei (en honor a Wei Dai).
- El precio del gas con relación a ETH es variable y son los mineros los que acuerdan subirlo o bajarlo. Se puede consultar en https://ethgasstation.info/

Fuente: https://respuestas.me/q/Cu-l-es-el-l-mite-de-gas-en-ethereum-25242288664

economistas
Colegio de Valencia

Características de un bloque Ethereum

- Se cierra un bloque aproximadamente cada 15 segundos.

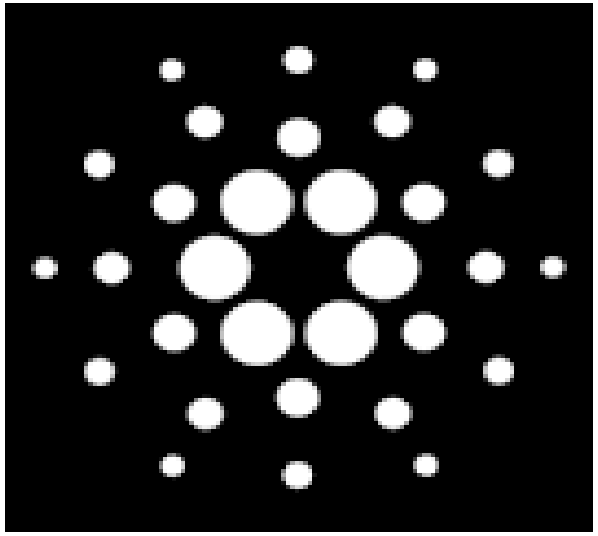
  https://etherscan.io/chart/blocktime
- El tamaño de bloque está fijado por el “límite de gas”.

  https://etherscan.io/chart/blocksize https://ethstats.net/
- Actualmente se cierra el bloque con el gasto de unos 8.000.000 gas.
- Las transacciones básicas (pagos de ETH de una cuenta a otra) tienen una complejidad de 21.000 gas.
- 8.000.000 / 21.000 = 380 transacciones, como mínimo, en un bloque.
- El tamaño de bloque es actualmente inferior a 30 KB.
- Información Ethereum en tiempo real: https://bitinfocharts.com/ethereum/

Fuentes: https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/

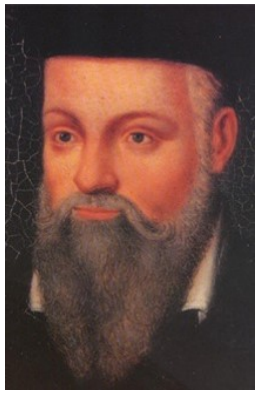
economistas
Colegio de Valencia

Cardano: la tercera generación blockchain



economistas
Colegio de Valencia

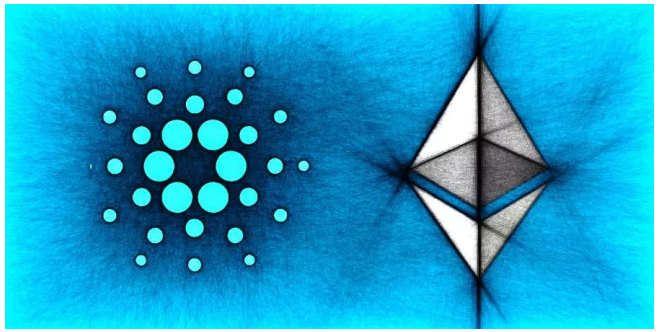
Cardano



- Plataforma distribuida creada por Input Output Hong Kong (IOHK) y dirigida por Charles Hoskinson, cofundador de Ethereum.

- Fue lanzada en septiembre de 2017.
- Su finalidad es la ejecución de smart contracts y aplicaciones descentralizadas.
- Ada es la criptomoneda asociada.

Fuente: https://en.wikipedia.org/wiki/Cardano_(platform)

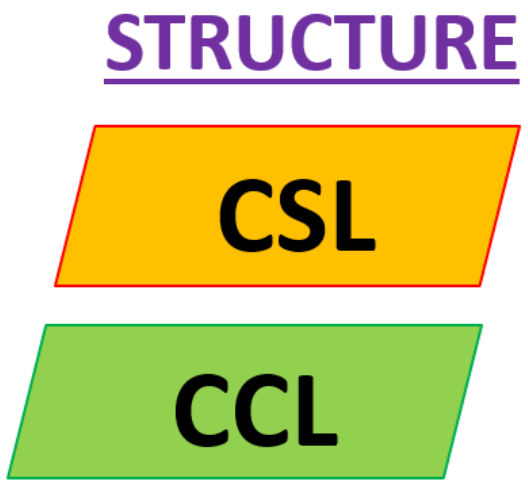


Cardano - II

- Las decisiones se toman a través de un algoritmo proof of stake llamado Ouroboros.
- Los nodos llamados “slot leaders” generan nuevos bloques en la blockchain y verifican las transacciones. Cualquiera que posea un Ada puede ser un slot leader.
- Utiliza una arquitectura multicapa.

Fuente: https://en.wikipedia.org/wiki/Cardano_(platform)
https://dollardestruction.com/4115/

Arquitectura en Cardano



- Cardano es una blockchain construida desde cero con una estructura diferente.
- Utiliza un lenguaje de programación funcional llamado Haskell.
- La arquitectura Cardano está desarrollada en dos capas:
  - CSL (Cardano Settlement Layer) es el ledger o libro de contabilidad que registra las cuentas para todas las transacciones.
  - CCL (Cardano Computation Layer) es la capa que funciona en base a la razón por la que se han producido las transacciones.

Fuente: https://steemit.com/cryptocurrency/@cryptolite/everything-about-cardano-2018

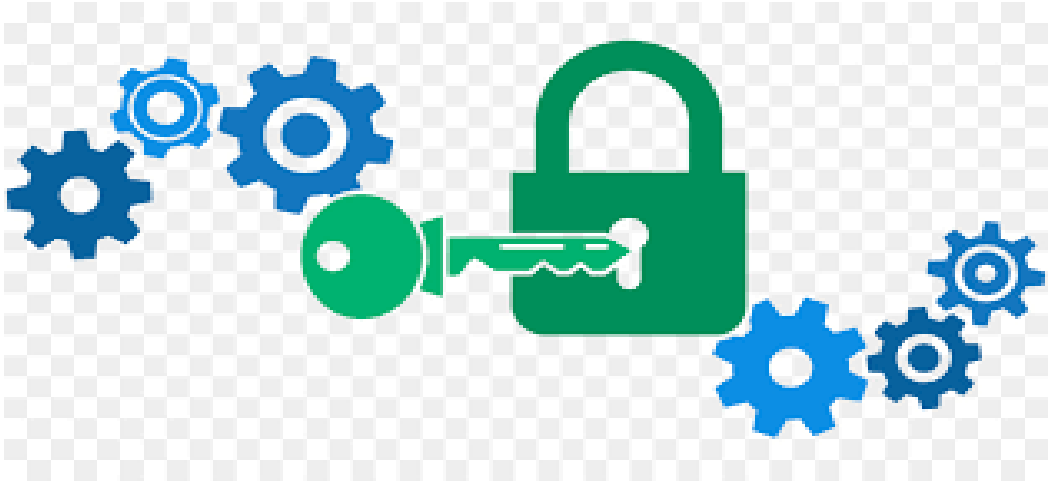
economistas
Colegio de Valencia

Sin Matemáticas no existiría Blockchain: Criptografía

Imagen: https://www.extremetech.com/extreme/214833-how-to-send-and-receive-encrypted-email-for-free

Criptografía

- Se asocia con el proceso de convertir texto plano en texto ininteligible y viceversa.
- Actualmente se ocupa de preservar en la información:
  - Confidencialidad
  - Integridad
  - No rechazo
  - Autenticación



Fuentes: https://economictimes.indiatimes.com/definition/cryptography

economistas
Colegio de Valencia

Funciones Hash

- Una función hash toma un conjunto de caracteres de longitud arbitraria y devuelve un conjunto de caracteres de longitud fija: 256 bits.

$$\text{SHA256}\,(\text{Hola mundo}) = \text{ca8f60b2cc7f05837d98b208b57fb6481553fc5f1219d59618fd025002a66f5c}$$

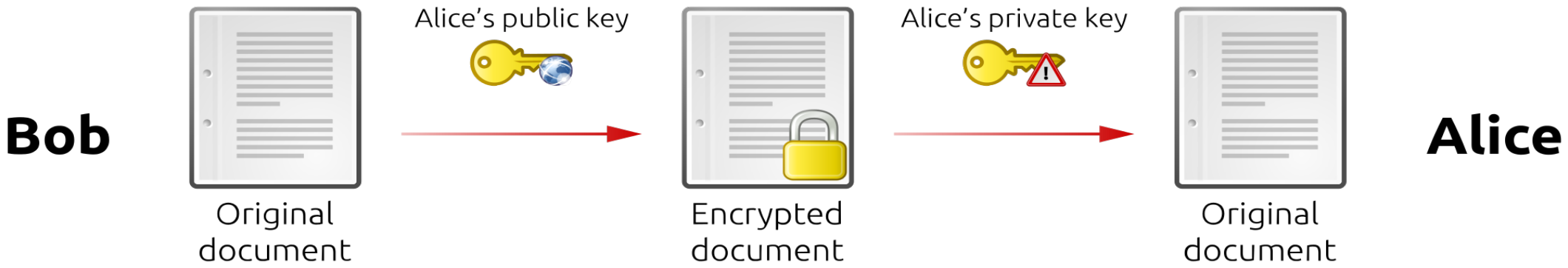
$$\text{SHA256}\,(\text{Hola mundo.}) = \text{8a3b7da2428acbc74623fb5a7b306a83b62b513371171e78c048fc12fbdb6ddf}$$

- Son funciones de un solo sentido, del resultado es prácticamente imposible obtener el dato original.
- Se puede utilizar para probar que algo es igual a algo, sin revelar de antemano la información.

Fuentes: https://learncryptography.com/hash-functions/what-are-hash-functions

Criptografía asimétrica

- Forma de encriptación en la que las claves se utilizan en pares: la clave pública y la clave privada.



Fuentes: https://commons.wikimedia.org/wiki/File:Asymmetric_Cryptography.svg

economistas
Colegio de Valencia

Para finalizar ...

- Preguntas
- Comentarios
- Sensaciones
- Preocupaciones
- ...

economistas
Colegio de Valencia

Gracias

Nuria de las Heras Santos

informática especialista en bases de datos y blockchain

nuria@nuriadelasheras.com
@n_delasheras
https://www.linkedin.com/in/nuriadelasheras/

Nuria de las Heras Santos

informática especialista en bases de datos y blockchain

nuria@nuriadelasheras.com
@n_delasheras
https://www.linkedin.com/in/nuriadelasheras/