Blockchain de café

DLTs para mi abuela

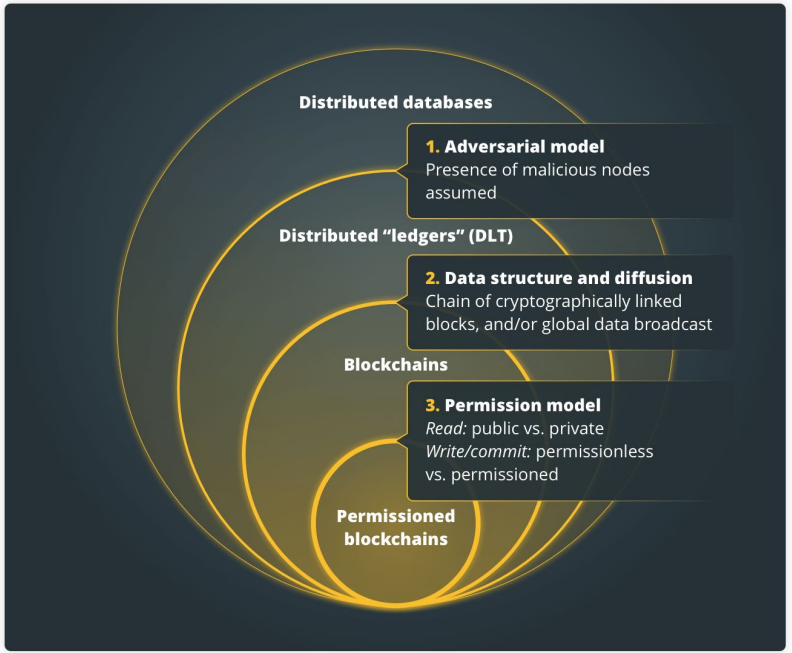
Agenda

- Qué es Blockchain, qué es DLT?
  - Introducción
- Cómo funciona?
  - Nodos y roles
  - Mecanismos de consenso
  - Interoperabilidad: Smart contracts, API, Oracles
- Use-cases:
  - Criptomonedas: Colateralización, descentralización, y eficiencia de capital
  - Blockchain Governance: integración de la industria 4.0
- Q&A

Introducción: Blockchain vs. DLT

- DLT = Distributed Ledger Technology
  - No hay administración centralizada
- Blockchain = Block + Chain
  - Los eventos se estructuran en cadena de bloques
- Blockchain es una forma de DLT
  - Se divide en nodos, que validan los eventos a través de consenso (no hay una administración centralizada)
- No todas las DLT son Blockchains
  - Aplicaciones específicas (ej. sistemas financieros, organización de “consorcios” entre sí, etc.)

The relationship between blockchain and DLT



cointelegraph.com

source: *jjablog*

Cómo luce un ledger?

TxHash	Block	Age	From	To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	0x8a91cac422e55e...	0.029594 Ether	0.000294

Hermoso, no?

Arquetipos de red

Tipos de DLTs: clasificación por privacidad

Ejemplos	Centralizada / Closed	Descentralizada / Open
Pública / sin permisos (permissionless)	**Sistemas de votaciones**	**Bitcoin**
Privada / restringida (permissioned)	**Sistemas de defensa/militares** **Sistemas impositivos**	**Supply chain** (todos pueden leer/trackear; sólo los suppliers pueden escribir)

Nodos: Clasificación

Por rol:

1. **Broadcast nodes:** solo “emiten” transacciones y se mantienen sincronizados con el estado actual
2. **Complete nodes:** inician y validan transacciones
3. **Mining nodes:** validan transacciones.
4. **Master nodes/supernodes:** Pueden iniciar eventos especiales (e.g. votaciones sobre mejoras del ecosistema), y pueden tomar decisiones si el consenso no se estabiliza.

Cómo se ponen de acuerdo para incorporar una nueva transacción?

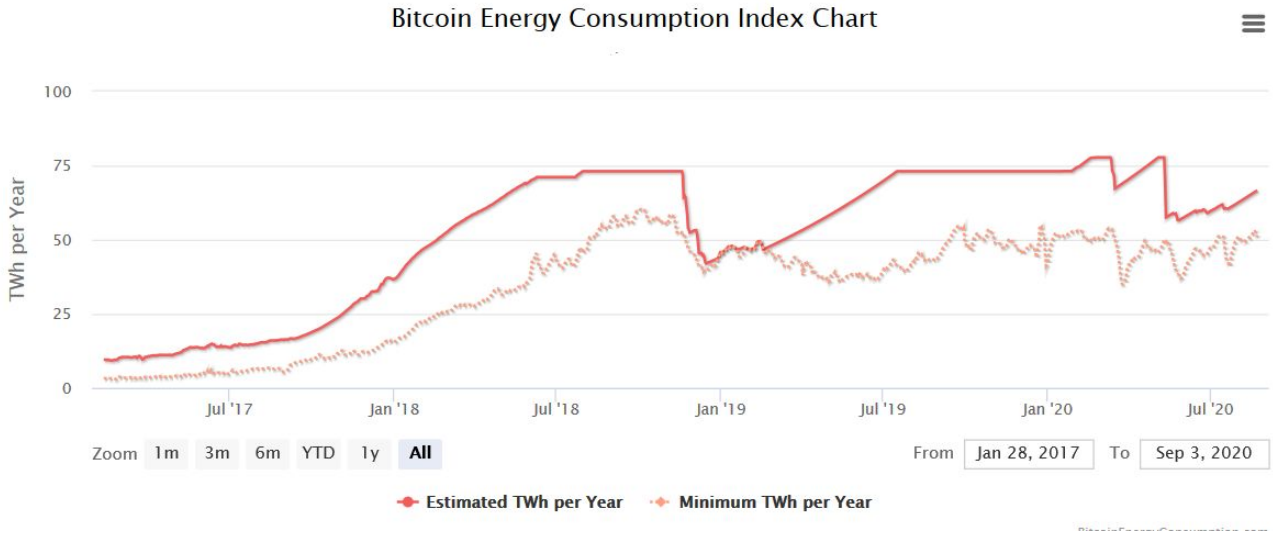
Mecanismos de consenso: la base de todo

El mecanismo de consenso intenta resolver la falla de los generales bizantinos

- Respecto a la DLT per se, es el motor de la validación
- En la capa de la arquitectura, es determinante en su naturaleza
- En la capa de infraestructura, establece los requerimientos de recursos
- En la capa de negocios, es la base de la confianza

Proof of Work (PoW)

Para validar un bloque, el minero debe resolver un “puzzle” matemático: es muy difícil resolverlo, y muy fácil verificar que se resolvió correctamente. El primero en resolverlo es el único que obtiene la recompensa. Desventajas:



Ref: Suiza consume 58,46 TWh por año

Fuente: Bitcoin Energy Consumption index, https://digiconomist.net/bitcoin-energy-consumption

Proof of Stake (PoS)

Cualquier usuario/agente/wallet que posea tokens son los que pueden validar nuevos bloques. El algoritmo elige “al azar” quién será el que valide y reciba la recompensa. La aleatoriedad está sesgada por diversos factores, pero principalmente por la cantidad de posesión, y por la longevidad de la posesión.

Ventajas: consume menos energía, e incentiva a los validadores a mantener la estabilidad de la red (al depender de la posesión de tokens).

- Actualmente, las DLTs más modernas utilizan una variante derivada, llamada Delegated Proof of Stake (DPoS), donde los delegados compiten en ofrecer servicios y mejoras para recibir los votos. Ha sido demostrado que el consenso se logra más rápido que en el PoS tradicional.

Interoperabilidad: smart contracts

Definición purista:

- Es un programa almacenado en un sistema DLT, sobre el cual cualquier resultado es registrado en su correspondiente distributed ledger.

Traducción para mi abuela (me tomo licencia poética por el simplismo):

- Cualquier software que se guarda en una DLT, y que permite hacer cosas en ella, siempre que los resultados se registren en dicha DLT.

Interoperabilidad: smart contracts

- En 2014, Ethereum fue el boom que llevó los smart contracts a las masas: los programadores comunes.

Use-case típicos académicos de smart contracts:

- Seguros: ej. Seguro de vida
- Supply Chain: Farmacéutica, Logística

Use-cases no tan típicos, pero más cerca de lo que la gente cree:

- Articulación de sistemas de información para IoT
- Inmuebles
- Registros de patentes, derechos, y propiedad (yapa: bancos de ADN)

Interoperabilidad: API

API = Application Programming Interface

Una API puede pensarse como un set de instrucciones para que otros programas utilicen y puedan operar sobre el sistema que hostea la API.

Ejemplo clásico de API en blockchain: plataformas de exchange

- Las API permiten la interoperabilidad tanto de sistemas puros como sistemas híbridos
- Promete ser la tendencia ganadora a largo plazo

Interoperabilidad: Oracles

Se llama oracle a todo sistema de información que permite interoperar sistemas basados en DLT con sistemas que no necesariamente son DLT.

Importancia: Permite reciclar los ya viejos y existentes sistemas EDI con sistemas de DLT.

- Ejemplo: Un seguro basado en una plataforma DLT (smart contract), que requiere el estado de un vuelo comercial en tiempo real. El oracle es quien le facilita la información de esa variable que no se encuentra en la DLT.

Criptomonedas: BTC y cía.

A diferencia de las stablecoins, el respaldo no se basa en justificar la emisión, sino en el equilibrio entre oferta y demanda.

Para ello se tiene que limitar la oferta: halving, dificultad de minado, tamaño del bloque, etc. Consecuencia: sistema financiero finito, pero volátil.

Por ello se adoptan mecanismos para atraer demanda y que supere la oferta (para generar efectos deflacionarios): ejemplo, fees de transacciones. Consecuencia: deflación (su valor aumenta con el tiempo), pero se hace más rentable cuanto más capital se maneja por transacción (le sale más caro a los que menor volumen manejan).

Criptomonedas: stablecoins

El gran trilema financiero:

- **Descentralización:** no existe autoridad central que valide las transacciones ni los eventos.
- **Eficiencia de capital:** las monedas requieren menos 100% de respaldo o menos del circulante.
- **Colateralización:** las monedas poseen un respaldo superior al 100% del circulante. El colateralizable es lo que permite a una criptomoneda utilizar valor de reserva/respaldo para estabilizarse, de ser necesario.

Ninguna stablecoin puede cumplir con las 3 propiedades. Siempre son 2 de 3!

Blockchain Governance: what?

Governance = decision making

El **WEF** propone un modelo de análisis de 3 capas:

1. Business Model = Negocios/Acuerdos
    a. Framework legal
    b. Sistema de incentivos para garantizar la confianza (“trust”)
2. Architecture model = Arquitectura
    a. Mecanismo de consenso
    b. Estructuración de la data de eventos
    c. Smart contracts
3. Infrastructure model = Infraestructura
    a. Configuración de nodos/red
    b. Eventos de la Blockchain

Blockchain Governance

- La industria 4.0 brinda una oportunidad única, de la mano de los digital twins, IoT, y DLT como una forma de tokenizar todo asset físico en un mundo digital.
- Tokenizar la economía global traería aparejados cambios radicales, tales como eliminar el contrabando, y facilitar la jerarquización de consorcios, entre otros.
- Liechtenstein es el país pionero, por ser el primer país del mundo en establecer la brillante ley TVTG (ley sobre tokenización, tokenomics, y token providers).

Blockchain Governance

- A medida que la complejidad de los sistemas aumentan, es crucial asegurar el control y la conformidad del mismo
- Esto es, establecer parámetros que permitan asegurar un framework sobre el cual se apliquen todos estos sistemas DLT
- Lo que hay en juego, hoy por hoy, es capital superior a los US$500Bn. Potencialmente podría ser la economía global, incluyendo información crítica y sensible de cada uno de nosotros!
- Sin governance, no hay garantías que la descentralización no termine resultando contraproducente.
- Por todo esto es que las instituciones de índole global como WEF, Davos Forum, ONU, y similares muestran preocupación por definir urgentemente estándares en blockchain governance.

Q&A: Gracias por la atención!