



Criptomonedas

October 2014

Criptomonedas

- Introducción
- Definiciones
- Historia
- Como funcionan
- Para que sirven
- Valoración
- Mercado
- Transacciones
- Opiniones



Introducción

- Esta presentación es de carácter **informativo**; no es una recomendación para invertir (o dejar de invertir) en Criptomonedas
- Existen muchas Criptomonedas en circulación; ciertas definiciones o comparaciones se hacen basados en las monedas mas comunes (*)
- El mercado, regulación y valor de las Criptomonedas cambia rápidamente; estadísticas y puntos de vista están basados en la información disponible al momento de preparar esta presentación



Definición

- Que es una Criptomoneda?
 - Es una “moneda” (originalmente *un medio de pago*) que **existe digitalmente** (no tiene representación física; no están ligadas a un activo físico) (*Moneda Digital, Digital Currency*)
 - Utiliza tecnología **criptográfica** para controlar su generación (creación), manejo y almacenamiento (e.g. para evitar que pueda ser copiada o alterada) así como registros digitales públicos encadenados (conocidos como “**blockchain**”) para control, uso y distribución.
 - **No son controladas** por un ente central o no cuentan con el respaldo de una entidad monetaria; se consideran un activo financiero descentralizado.



Definición

Moneda “Tradicional” (USD, COP, CAD,...)	Criptomoneda (Bitcoin, Ethereum, ...)
Emitida por un gobierno/país o entidad monetaria	Creada por desarrolladores / programadores; generalmente existe una definición publica acerca del funcionamiento de la moneda
Cuenta con el respaldo y regulación de una entidad especifica así como organismos internacionales; tiene un esquema de control mucho mas robusto	No tiene un ente regulatorio centralizado; se rige por parámetros definidos por los programadores y/o en el diseño de la moneda virtual.
Representada físicamente (billetes, monedas) emitidos por un ente central	Totalmente digital (creación, uso, almacenamiento, transferencia)
Emisión de moneda puede ser ilimitada	Ciertas Criptomonedas* tienen un máximo de unidades; así mismo existen reglas para la creación de nuevas unidades o el proceso de asignación de unidades a usuarios
Pueden percibirse como mas estables (monedas fuertes), sin embargo no es siempre el caso (hiperinflación/devaluación)	Alta volatilidad y sujetas a variaciones de oferta/demanda así como percepción de “valor”
La moneda física (cash) no necesita tecnología para su uso o distribución	Requieren de una plataforma tecnológica para existir y funcionar



Historia

- El concepto de **monedas digitales** existe desde la década de 1980; varios intentos ([DigiCash](#), [eGold](#)) fracasaron por diversas razones (regulación, fraude, adopción limitada,...)
- Medios electrónicos de Pago (e.g. Paypal) crearon mecanismos exclusivos para transferencias dentro de sus redes sin embargo no alcanzaron un uso generalizado



Historia

- En Octubre del 2008, el concepto de “**Bitcoin**” (*peer-to-peer electronic cash system*) fue inicialmente propuesto en un documento escrito bajo el seudónimo de “**Satoshi Nakamoto**”
- No se sabe la identidad real o la ubicación actual del autor(es)
- La propuesta creó simultáneamente la primera “**blockchain**”

https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf



Historia

- Después de BITCOIN, se han creado **cientos** de monedas, generalmente llamadas “**AltCoins**” y que siguen protocolos similares a BitCoin
- Los **Tokens** (Fichas) se basan en tecnología blockchain y representan una “unidad de valor”, se usan mas para contratos y transacciones

CriptoMoneda



ALT Coins
(Monedas Alternativas)

Stable Coins
(Moneda Estable)

Tokens
(Fichas)



Como funcionan?

- Las Criptomonedas se basan en la tecnología “**blockchain**” o registro digital encadenado, en la cual transacciones son agrupadas en **bloques**, registradas de manera distribuida en **múltiples** nodos de la red y vinculadas entre si utilizando **claves únicas (encriptadas) de identificación** (“hash”)



Cómo funciona:



Alguien solicita una transacción.

La transacción solicitada es transmitida a una **red punto a punto (P2P) conformada por computadoras, conocidas como nodos.**



Validación

La red de nodos **valida la transacción y el estado del usuario usando algoritmos conocidos.**



Una transacción **verificada** puede contener **criptomonedas, contratos, registros** u otra información.



La transacción **esta completa.**



El nuevo bloque es el agregado a la **cadena de bloques existente, de forma permanente e inalterable.**



Una vez que la transacción es verificada se combina con otras transacciones **para crear un nuevo bloque de datos para el registro.**



Como funcionan?

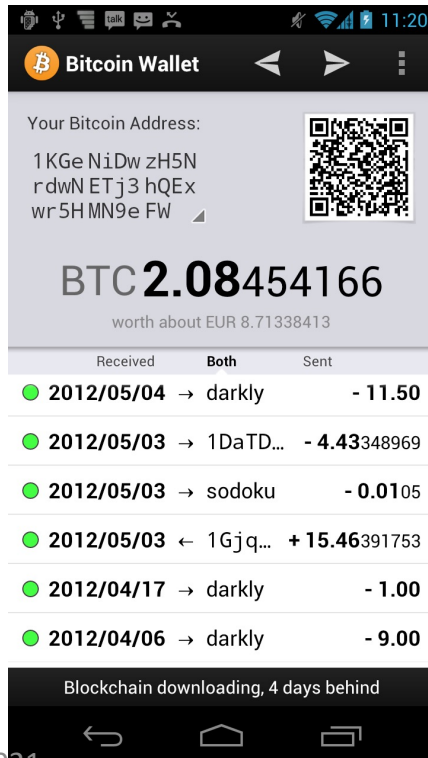
- Al no existir un entidad central, los **nodos** de la red que soportan la cadena así como la creación de nuevos bloques de transacciones son realmente usuarios privados (personas o compañías)
- Ciertas* monedas recompensan a los nodos con un porcentaje de nuevas Criptomonedas, ya sea por mantener la red o por procesar nuevas transacciones. Esto se conoce como “**cryptocurrency mining**”
- Para hacer “**mining**” se requieren de equipos de computación y programas especializados así como de costos de operación (energía)
- Ciertas* Criptomonedas tienen un limite (BITCOIN = 21 Millones de Unidades) definido previamente en los algoritmos de generación



Como funcionan?

- Dado que las Criptomonedas son puramente **digitales**; necesitan ser almacenadas en medios electrónicos, ya sea “online”, “offline” o en ciertos casos, imprimiendo los códigos de validación & identificación. Existen muchos proveedores de “**digital wallets**”

HOT
(Online)



COLD
(Offline)



Paper
(Printed)



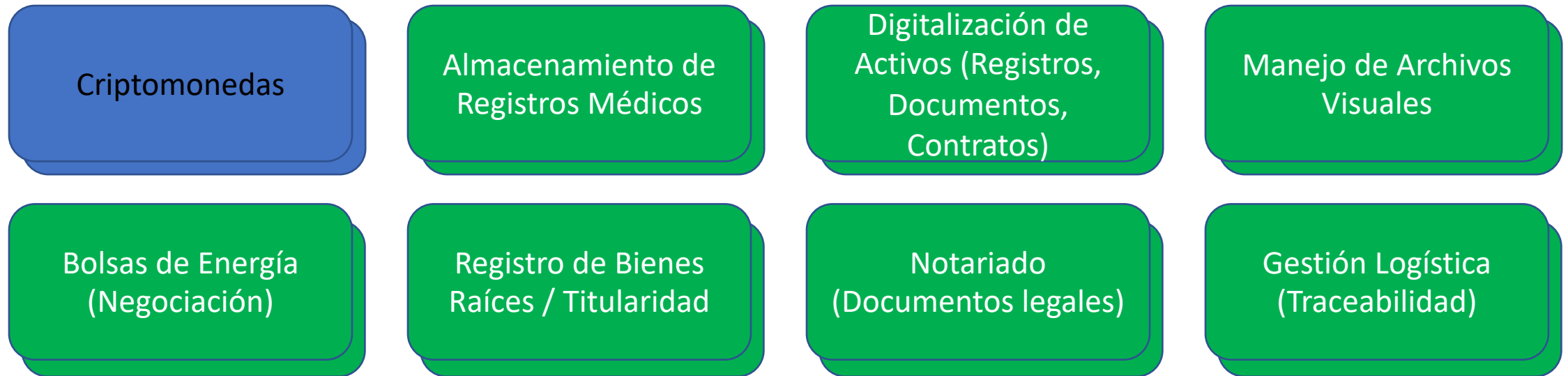
Para que sirven?

- El concepto de Digital Currency (monedas Digitales) nació *primordialmente* como un **mecanismo de pago** para transacciones digitales entre personas; la premisa original es:
 - Eliminar (reducir) el costo de transacciones
 - Eliminar intermediarios financieros (=bancos)
 - Disminuir el tiempo necesario para ejecutar una transacción
- Algunos promotores de las Criptomonedas indican otros *beneficios**:
 - Protección contra la Inflación
 - Almacenamiento de Valor (Assets)



Para que sirven?

- Aunque las Criptomonedas reciben muchísima atención, la tecnología **blockchain** ha generado un numero **mucho mayor** de usos potenciales:



Valoración

- Las Criptomonedas **no** tienen un valor intrínseco
- Conceptualmente, el valor de una Criptomoneda estaría definido por
 - el balance entre la oferta y demanda
 - los casos de uso que generen (valor agregado)
 - el esfuerzo para su generación
 - para ciertas monedas (StableCoins), el valor del activo al cual están alineados
 - el valor que un usuario esta dispuesto a pagar



Valoración

- En la realidad, existen muchos factores que han afectado (y afectan) el valor percibido de una Criptomoneda:
 - Los prospectos de que dicha moneda (o Blockchain) sea ampliamente usada (*adopción y uso*)
 - La imposición de regulaciones que limiten, faciliten o amplíen el uso de una moneda (*eg. China, El Salvador*)
 - El soporte tácito o real de organizaciones o compañías en el uso de Criptomonedas (*e.g. Tesla, MicroStrategy, PayPal*)
 - Influencias **externas** a las fuerzas naturales del mercado



Mercado

- Bitcoin fue la primera Criptomoneda y ha logrado alcanzar un mercado representativo (tanto penetración & uso); hoy en día representa el ~50% del **mercado** (>95% en 2015)
- Existen cientos de Criptomonedas (“coins”) así como “tokens” construidos a partir de los conceptos fundamentales de **BlockChain**
- El Mercado de las Criptomonedas se estima en **\$2.0 Trillones de dólares***

<https://markets.bitcoin.com>

<https://coinmarketcap.com/all/views/all/>



Transacciones

- Existen diferentes mecanismos para adquirir, vender o intercambiar Criptomonedas:

P2P	ATM	Bolsa de Monedas (Coin Exchange)	Online Brokers (Acciones)
<ul style="list-style-type: none">• Proceso “original”• Transacción directa entre 2 personas• Alto riesgo en caso de no conocer a la contraparte	<ul style="list-style-type: none">• Funciona como un cajero automático	<ul style="list-style-type: none">• Permite comprar múltiple Criptomonedas• Pueden servir como almacenamiento o transferirse a billeteras digitales	<ul style="list-style-type: none">• Permite comprar monedas, acciones, derivados• Negocios establecidos y con presencia en mercado de acciones
<ul style="list-style-type: none">• Requiere Billeteras Digitales• No se puede reversar	<ul style="list-style-type: none">• Disponibles solo en ciertas áreas/países• Requiere Billeteras Digitales	<ul style="list-style-type: none">• Varias opciones disponibles• Pueden tener riesgos adicionales (hackers)	<ul style="list-style-type: none">• Muchas opciones disponibles con diferentes mecanismos de seguridad, almacenamiento



Opiniones

- Existen muchos puntos de vista y opiniones acerca de los **riesgos, ventajas y desventajas** de las Criptomonedas:

+

- Elimina el control de entidades financieras
- Reduce costos de transacción
- Manejo descentralizado (DeFi)
- Ajenos a manipulación monetaria
- Protege contra inflación
- Almacenamiento de valor (activos)
- Todas las transacciones son registradas
- Es el futuro de la moneda

-

- Facilita transacciones anónimas / ilegales
- Requiere acceso a tecnología
- Falta de control unificado
- Sensible a manipulación de mercados
- Alta volatilidad
- Falta de Valor de respaldo
- Anonimato & marco legal indeterminado
- Inestabilidad legal puede limitar crecimiento



Foro de discusión

- Eventos recientes & notables en la historia de Criptomonedas
 - La influencia de personalidades en el comportamiento del mercado
 - [Impacto](#) de tweets de Elon Musk en valoración de ciertas monedas
 - Adopción por parte de compañías reconocidas ([Microstrategy](#), PayPal, tesla)
 - Contrastes en torno a regulación
 - China declara Criptomonedas como [ilegales](#); lanza el [DigitalYuan](#)
 - [El Salvador](#) declara Bitcoin como su moneda legal
 - Cual es el futuro de las Criptomonedas?
 - Incremento en la regulación y control? (eliminar anonimato)
 - Adopción generalizada en el mercado: el boom de nuevos inversionistas?
 - Es la entrada de entidades financieras tradicionales (bancos & bolsas) al mercado una señal de aprobación o simplemente una manera de no quedarse por fuera?



Gracias