Blockchain:
criptoactivos

Carlos Castro-Iragorri

Clasificacion

Token digital (Lewis, A. 2018)

Ficha cuyo valor depende del contexto y que utiliza un mecanismo de autenticación digital (PKI).

- Nativos: hacen parte fundamental del protocolo de un blockchain.
- Respaldados por un activo(s) físicos.
- *Utility*: permiten reclamar un servicio del emisor.

Tokens nativos

- Usualmente conocidos como “criptomonedas”. Valor intrinseco.
- Hacen parte del mecanismo de incentivos.
- Mecanismo de pago aceptado en el blockchain.
- Reglas definidas en el protocolo.
- BTC, ETH, NXT, XPR,…

BTC

- “Moneda” (activo digital) cuyas transacciones (cambios de propiedad) quedan registrados en la Bitcoin Blockchain (registro).
- Innovación: permite intercambio digital (vs físico) entre A y B sin requerir intermediarios específicos (terceros).
- *“Primer dinero digital que es resistente a la censura”*, Tim Swanson

Registro digital de transacciones

Tradicional

1. Administrador centralizado
2. Asignación e identificación cuentas
3. Registro centralizado (reconciliación).
4. Orden de los registros.
5. Único creador de registros.
6. Mandato para crear registros.
7. Índice de los registros

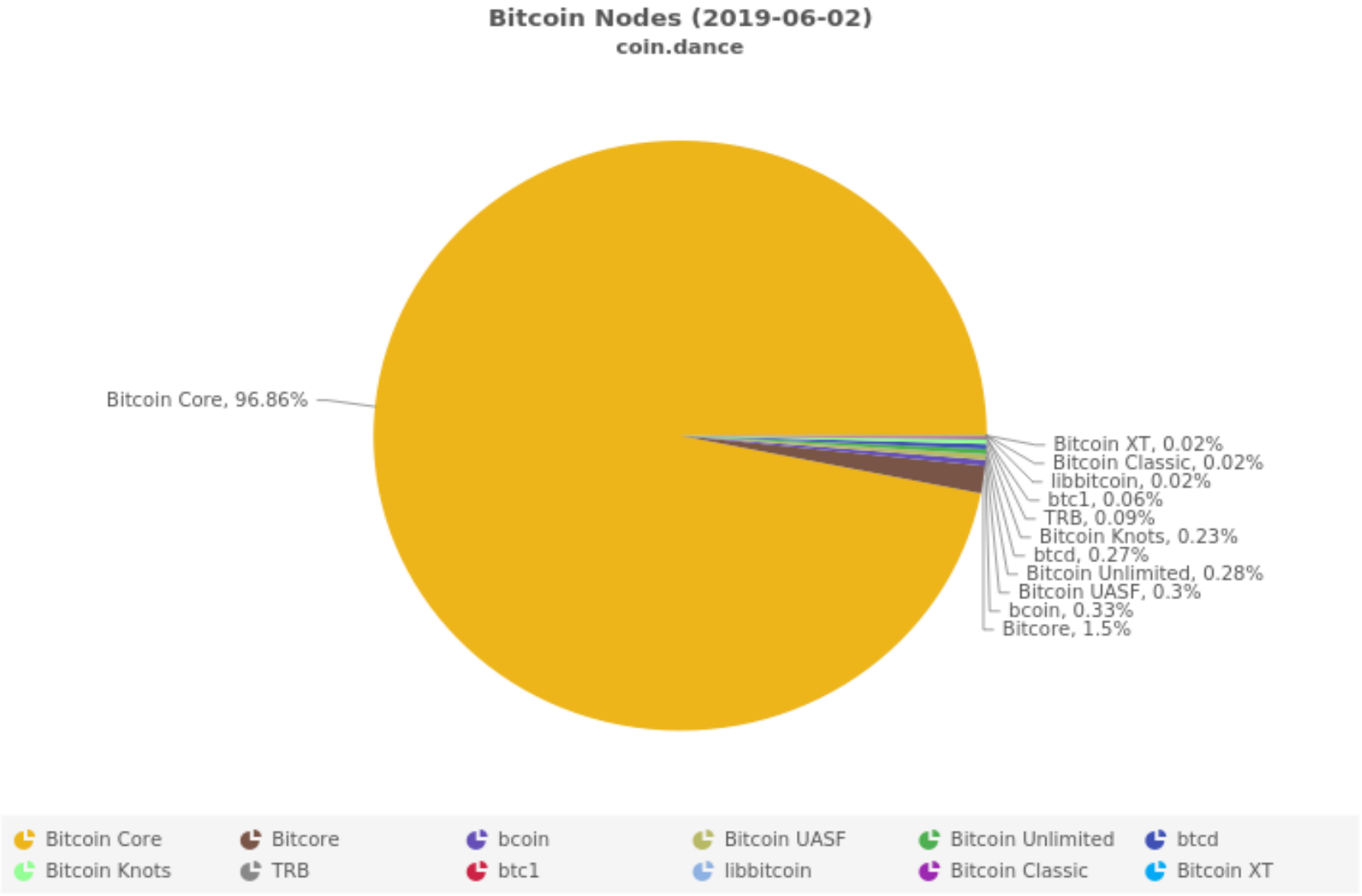
BTC

1. Ecosistema distribuido
2. PKI
3. Registro distribuido.
4. Bloques.
5. Varios mineros con mecanismo de coordinación POW.
6. Incentivos para crear registros (pagos): minado y transacciones.
7. Encadenamiento.

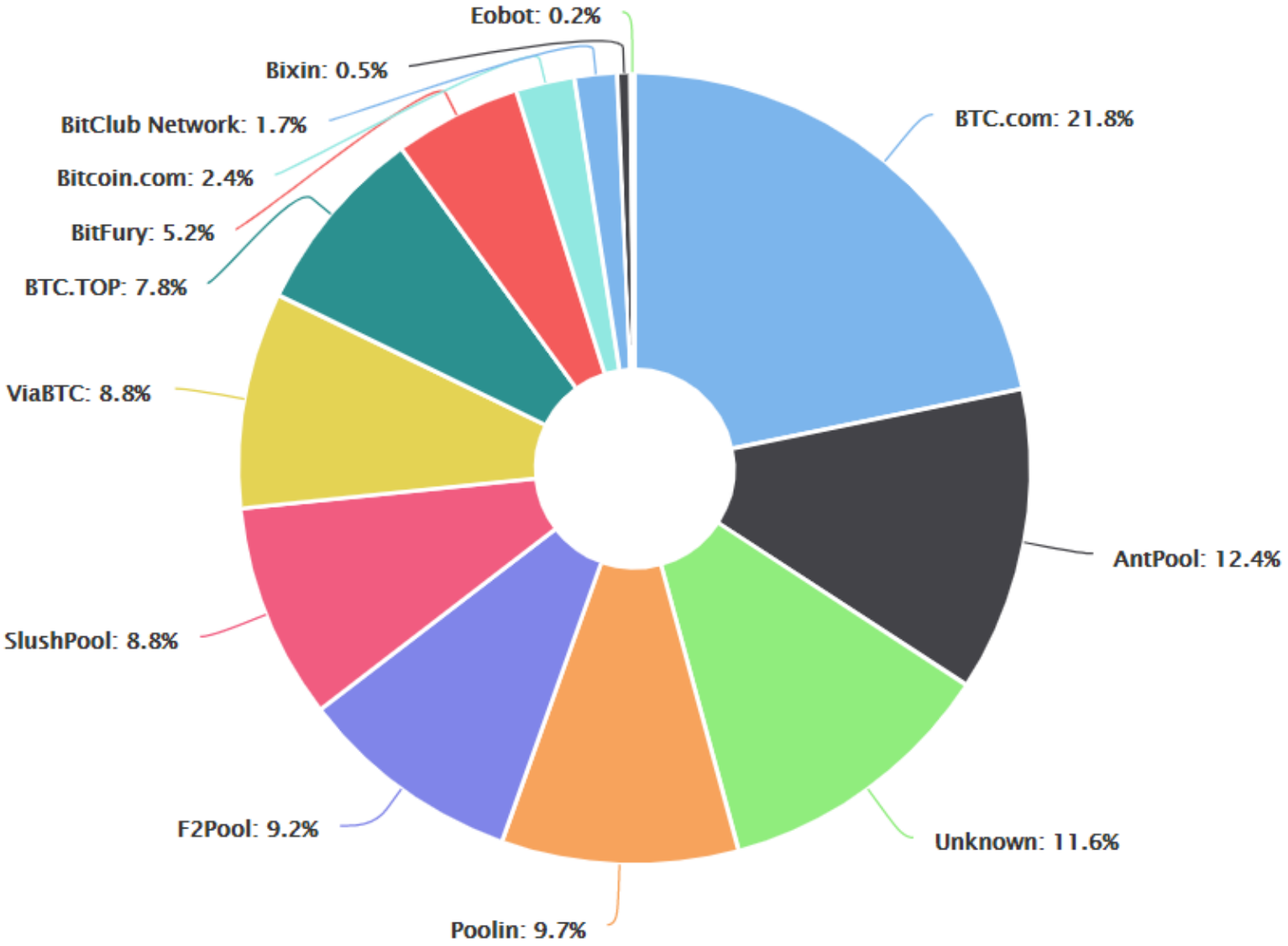
Características del minado

- Creación de nuevos bloques +- 10 min.
- Pago por minado mecanismo para iniciar el blockchain, converge a 0 sustituido por pagos por transacciones.
- 2009-2012 (50), 2013-2016/07(25), 2016-2020(12.5)…2140 (0).
- BTC circulación 17M de 21 M (81%).
- Política Monetaria: Autobalance entre la dificultad de crear nuevos bloques y velocidad a la que se crean.

Gobernanza del protocolo



Nodos de minado, 80% China



ETH

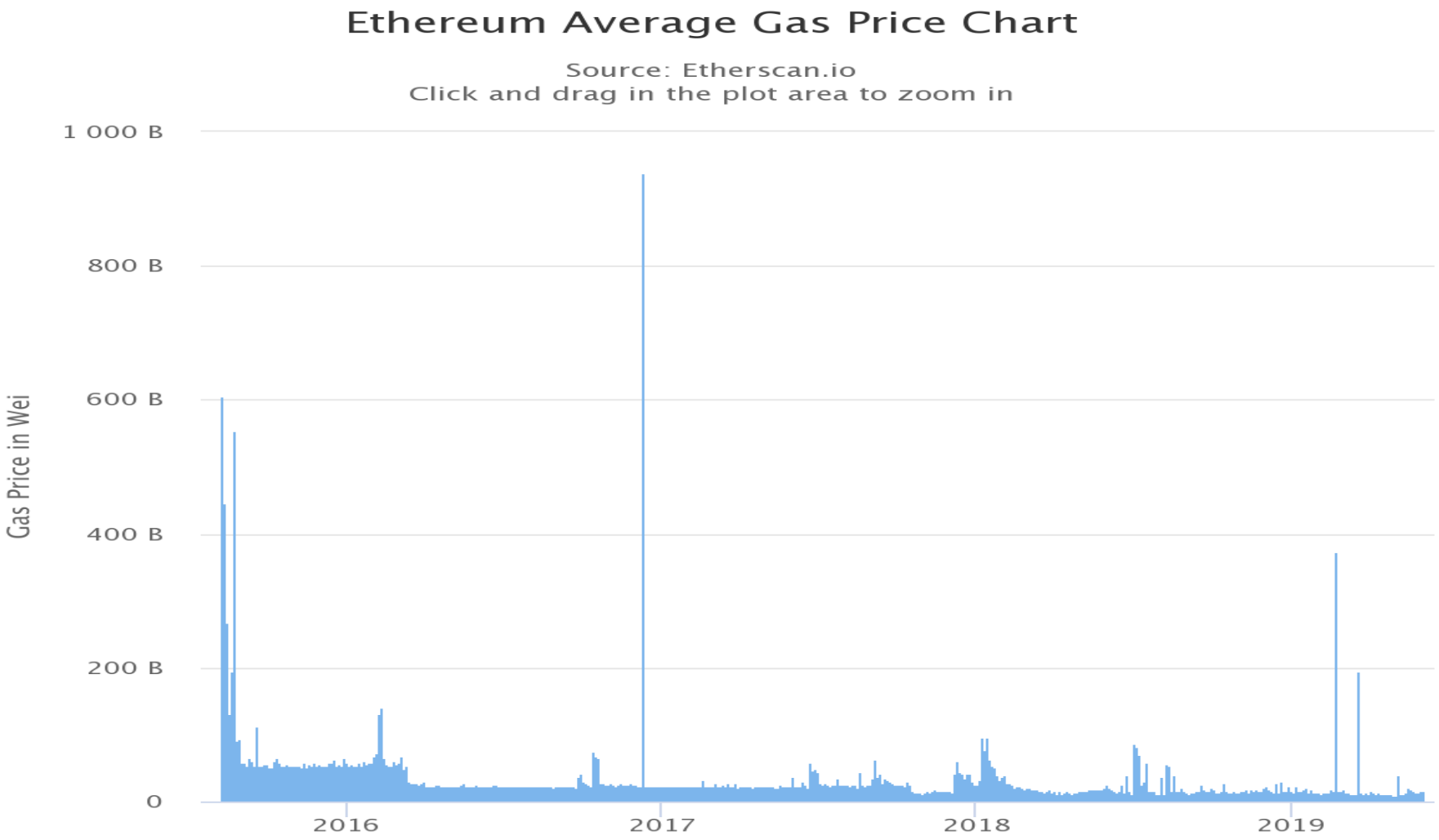
Computador descentralizado, sostenible y resistente a la censura. Permite almacenamiento de datos y procesos.

- Ether para ejecutar Contratos Inteligentes en los nodos.
- Sin permisos pero también se puede utilizar permisionada (Enterprise Alliance).
- Creación de bloques: POW → POS (ETH en Balance para minería).
- Pago por transacción (depende de la complejidad): Gas

Precio operación en la red

Operation Name	Gas Cost	Remark
step	1	default amount per execution cycle
stop	0	free
suicide	0	free
sha3	20	
sload	20	get from permanent storage
sstore	100	put into permanent storage
balance	20	
create	100	contract creation
call	20	initiating a read-only call
memory	1	every additional word when expanding memory
txdata	5	every byte of data or code for a transaction
transaction	500	base fee transaction
contract creation	53000	changed in homestead from 21000

Precio Gas


Ethereum Average Gas Price Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
1 000 B
800 B
600 B
400 B
200 B
0
Gas Price in Wei
2016
2017
2018
2019

Podemos considerar BTC como dinero?

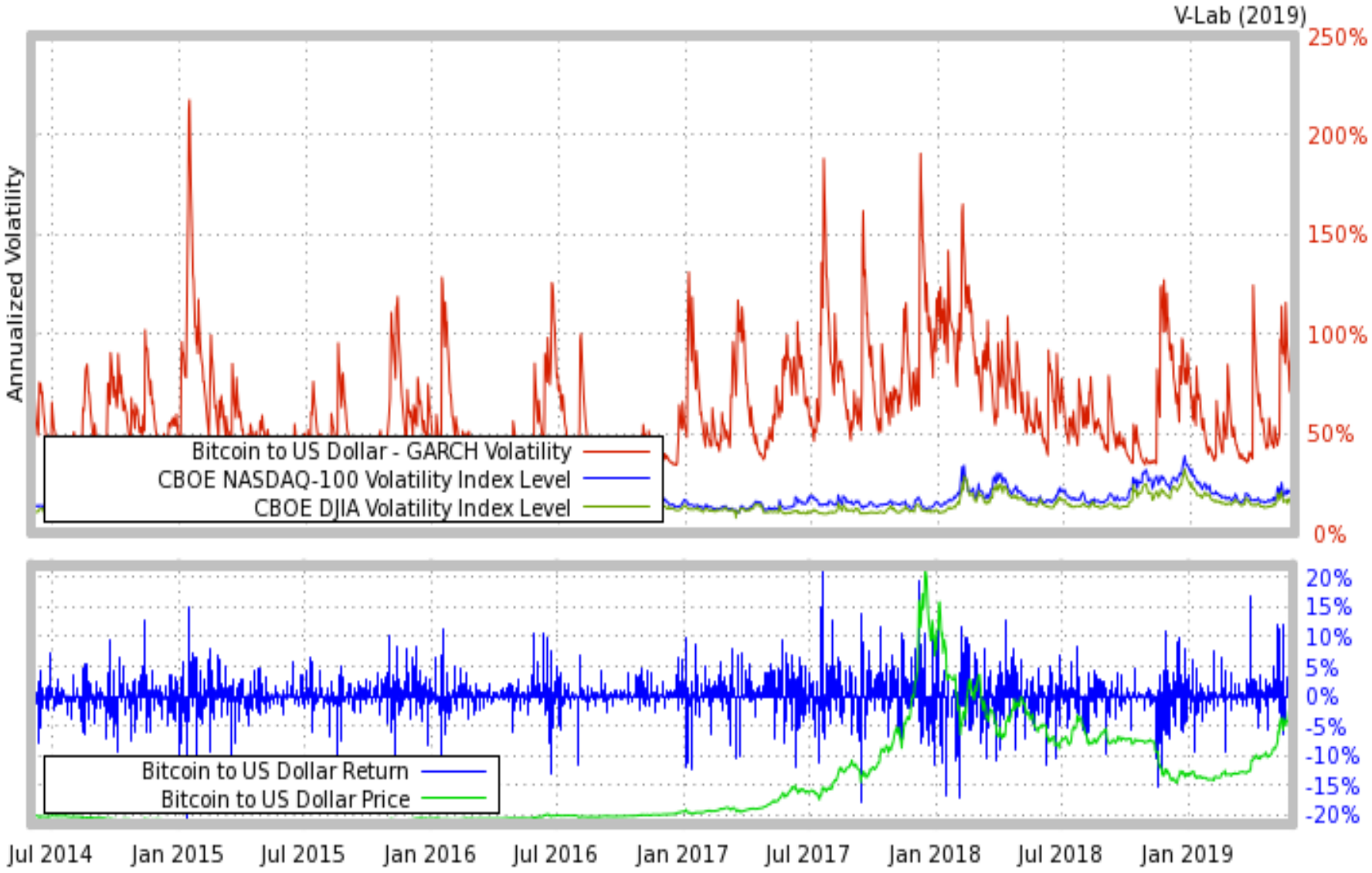
Dimensiones del dinero (digital)

- Medio de intercambio/pago, aceptado (jurisdicción).
- Deposito de valor (envilecimiento / inflación).
- Unidad de medida (*numéraire*).
- Dinero físico: anónimo, sin intermediario, no funciona para transacciones a distancia.
- Dinero digital: identificación, intermediarios (registros, canales de comunicación), transacciones a distancia pero complejas (excepto pagos).

BTC y las dimensiones

- Medio de intercambio:
  - Adopción irregular y baja. Solo 1.3% transacciones en el registro son de pagos por bienes y servicios (2019).
  - No hay eliminación de intermediarios, Exchanges.
- Deposito de valor y unidad de medida: Si uso es principalmente especulación entonces es altamente volátil y por va en contravía.
  - Valorización importante.
  - Costos de menú altos.
- *“ha fracasado en estos aspectos”*, Carney M. BoE.
- Excepto por resistencia a la censura: estado fallidos.

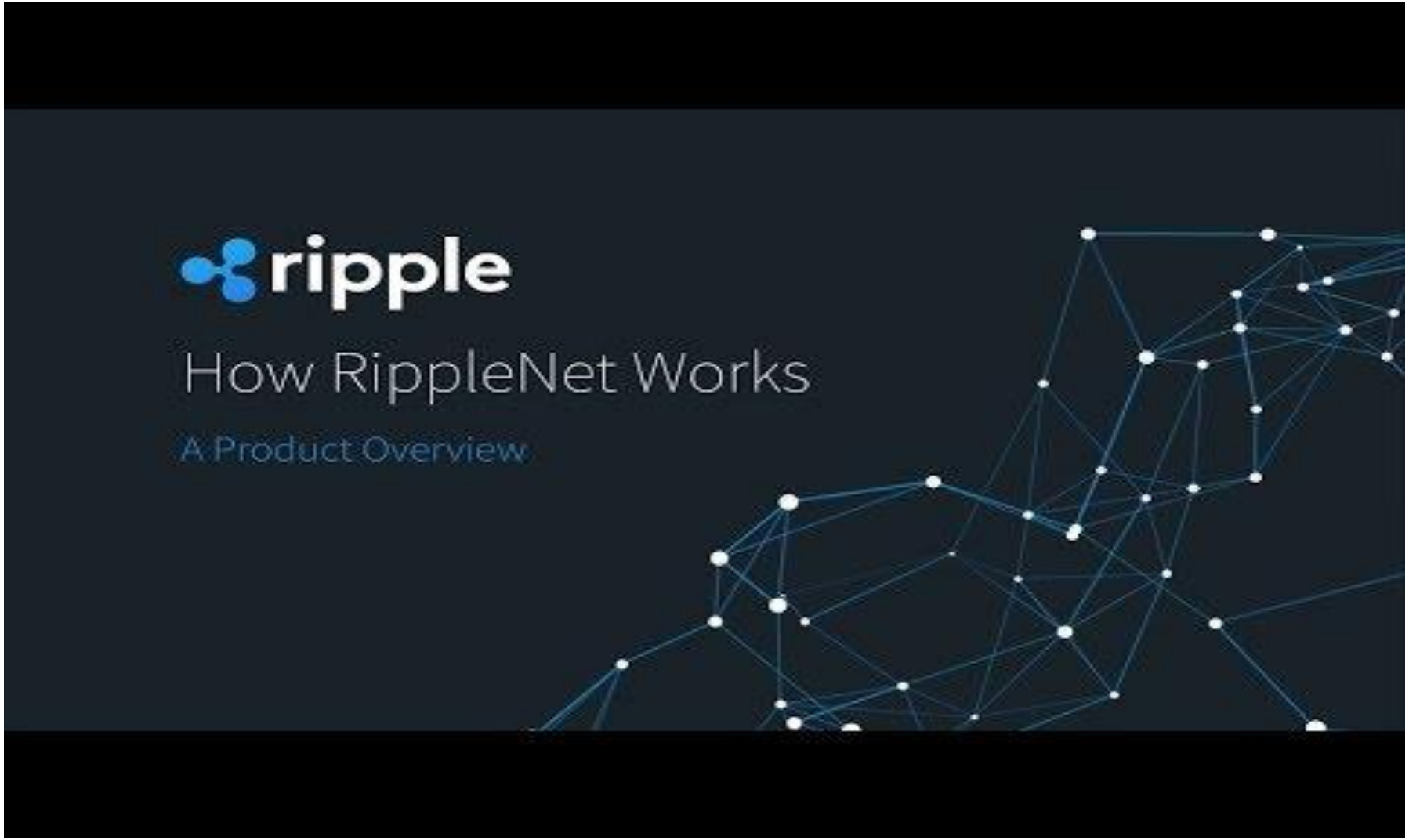
Volatilidad BTC



Precursores a BTC

- Digicash (1983). Pagos comercio y bancos, comercialmente fracaso 1998 (NL).
- B-money (1998). Transacciones anonimas.
- Hashcash (1992). Pagos por *“junk mail”.*
- e-gold/Liberty reserve (1996). Unidades digitales respaldadas por oro, centralizado, cerrado por fraude y facilitar actividades ilicitas.

Ripple, pagos internacionales



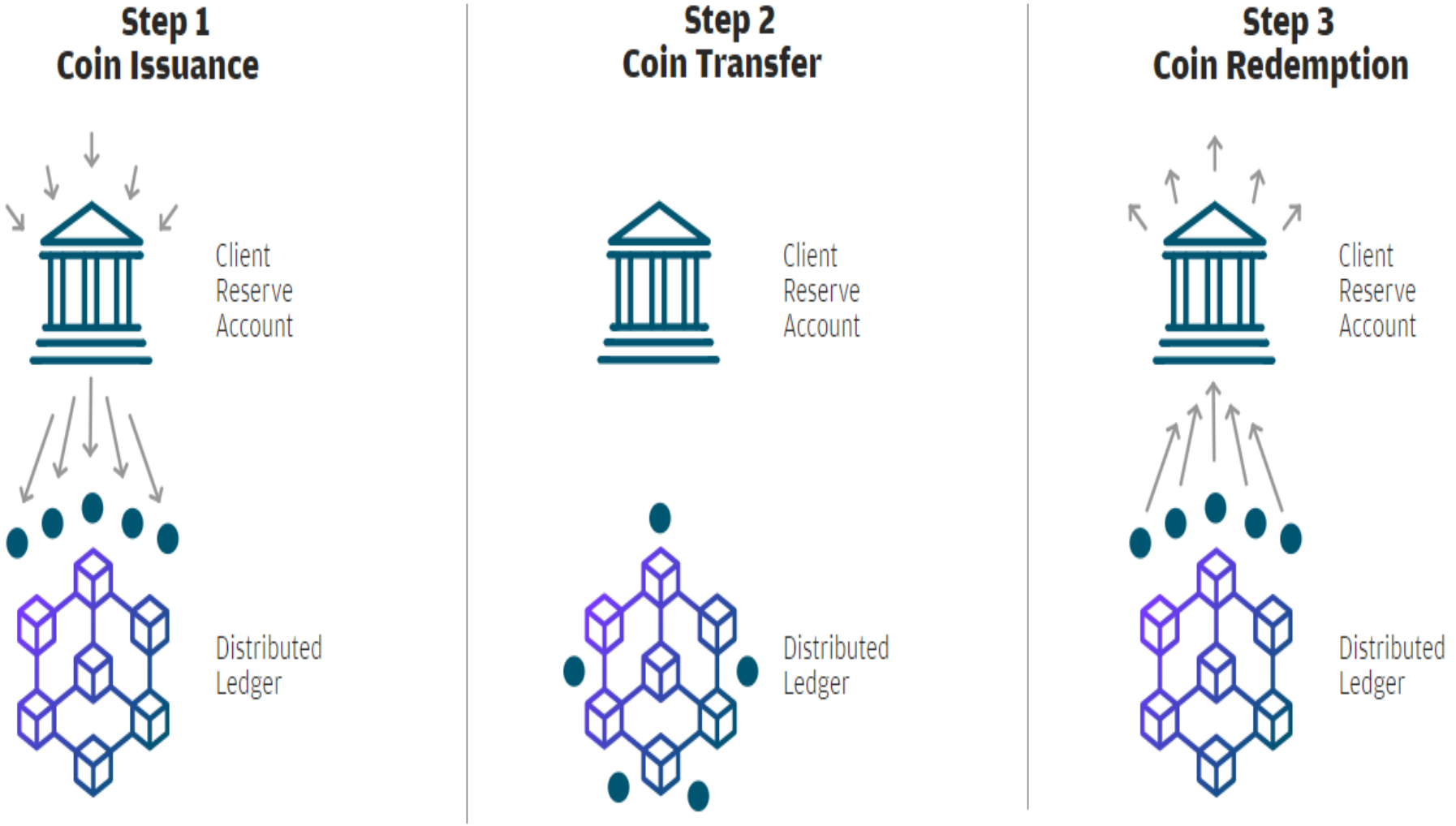
Tecnología alternativa, Revolut, 2015

- Fintech / Mastercard pre-paid.
- Banco global de pagos y transferencias.
- Tarjeta de viajero sin costos de intercambio entre monedas (hasta cierto valor).
- Permite comprar criptoactivos.
- Crecimiento importante en Europa, >1M de usuarios y 42M transacciones.

JP Morgan Stable Coin, Feb 2019

- Moneda para hacer pagos en diferentes monedad, JPM Coin.
- Tecnología Blockchain, Quorum, extendible a otras.
- Mantiene equivalencias con las principales monedas a nivel mundial.
- Clientes intitucionales

JP Morgan Stable Coin, Feb 2019



Banca Central y Blockchain

- Pilotos de moneda digital emitida por bancos centrales.
- Transferencias interbancarias sobre registro distribuido.
- Redes permisionadas
- Corda, Fabric, Quorum, Ethereum (permisionado)
- Wholesale / Retail CBDC.

Otros Tokens e ICOS

Tokens respaldados por activos

Token representa un activo financiero o un derecho sobre un activo que puede ser emitido por un custodio.

- Certificados de deposito sobre un subyacente físico u activo financiero guardado por un custodio.
- Titulo, prueba de propiedad no hay custodio.
- Contrato, obligación contractual y directa del emisor (no en el sentido de custodio).

Beneficios de la tokenizacion

- Criptografía ofrece resistencia falsificación.
- Eficiencia en el proceso de emisión e intercambio: registro compartido.
- Segregación de responsabilidades.
  - Intercambio
  - Custodio
- Beneficios de la competencia.
  - Actualmente integración vertical por beneficios operativos.
  - Ofrecer un registro y estándares que permitan la entrada de mas oferentes.

Tokens que prometen un producto o servicio

Token que provee una utilidad permitiendo reclamar un producto o servicio especifico.

- Pasivo del emisor (servicios por prestar o productos por entregar).
- Mecanismo popular en las ICO’s y similar a plataformas de crowdfunding.

Crowdfunding

Sistema de financiación directa, no localizada, no especializada en las etapas tempranas de un proyecto.

- Pre-venta
- Préstamo
- Donación
- Capital social

Regulación: registro, topes (aportante individual y financiación total), provisión de información, periodo mínimo de inversión, independencia (plataforma / proyectos).

Han creado un mercado secundario.

Initial Coin Offerings

- Nueva forma de recaudar fondos.
- Descripción producto o servicio (whitepaper/prospecto), junto con emisión de token.
  - Acceso a producto / servicio.
  - Activo financiero (no necesariamente acciones)
- Evitar ser clasificado como activos financieros.
- Menor plazo entre fondeo inicial con inversionistas privados a ser listados en mercados.
- Inmediatamente pueden ser transados.
- Oportunidades de inversión compañías "privadas".

Test Howey, 1964

1. Inversión en dinero u otros activos.
2. Expectativa de retornos sobre la inversión.
3. Inversion es alrededor de un proposito comun.
4. Retornos vienen del esfuerzo de un promotor o tercero.

https://www.revolut.com/

Calsificacion FINMA, 2018

	Pre-financing and pre-sale / The token does not yet exist but the claims are tradeable	The token exists
ICO of payment tokens	= Securities ≠ subject to AMLA	≠ Securities = means of payment under AMLA[3]
ICO of utility tokens[4]		≠ Securities, if exclusively a functioning utility token = Securities, if also or only investment function ≠ means of payment under AMLA if accessory
ICO of asset tokens[4]		= Securities ≠ means of payment under AMLA