# Criptodivisas, Bitcoin y Seguridad

Miguel A. Ortuño Pérez
Escuela Técnica Superior de Ingeniería de Telecomunicación

http://gsyc.urjc.es

Febrero de 2016


http://ortuno.es
@MiguelOrtunoP

# Contenidos

# Criptodivisas: el bitcoin

El bitcoin ya forma parte de nuestra sociedad, aunque sea como una anécdota en la prensa sobre inversores temerarios
Son frecuentes opiniones como esta:

- *Creer que el resolver unos problemas matematicos crea valor es como creer que mis crucigramas resueltos en viejas revistas pueden hacerme rico. El dinero tiene valor por que hay algo que lo respalda poco o mucho. Bankia o el estado algo tienen. Tus criptomonedas y tus problemas matématicos para mi, como para el 99,99 % de la sociedad no valen nada, o valen tanto como mis sopas de letras* [1].

Las criptodivisas tienen puntos fuertes y puntos oscuros, pero veremos que argumentos como este, son muy débiles

[1] spqr2004, elmundo.es, febrero 2014

# El dinero no es la riqueza

Dinero y riqueza son conceptos muy distintos

- Cuando un gobierno tiene problemas económicos, tiende a *imprimir* más dinero ¿resuelve el problema?
- Zimbawe, década de 2000. Todo el mundo era millonario y muy pobre. Inflación de millones por ciento, una barra de pan costaba billones de dólares zimbaweses

Fenómeno de la *Ilusión monetaria*:

- Una bajada de sueldo del 5 %
- Una subida de sueldo del 5 %, con subida de precios del 10 %

Ambas cosas resultan prácticamente equivalentes, pero está demostrado que la mayoría de las personas perciben lo primero como mucho peor. Casi todo el mundo piensa en términos nominales, no en términos reales

# Trueque y dinero

Antes del dinero, existía el trueque
*Te cambio mi gallina por tu saco de manzanas*
Problemas:

- ¿Y si yo no quiero manzanas?
- ¿Y si yo solo quiero dos manzanas? ¿Cómo troceo la gallina (sin matarla)?
- ¿Y si quiero guardar las manzanas varios meses?

Aparecen trueques más complejos usando algún bien intemedio como sal, tabaco, cacao, metales.
Dinero es *todo medio de intercambio común y generalmente aceptado por una sociedad que es usado para el pago de bienes, servicios y obligaciones*[2]

[2] wikipedia.es

# El oro como dinero

El oro siempre ha sido un buen dinero:

- Tiene valor intrínseco (ornamental e industrial)
- Es duradero
- Es transportable
- Es divisible, y las divisiones se pueden recomponer
  - Piezas diferentes se pueden fundir en una sola
  - A partir de una aleación, con ácido nítrico se puede recuperar el oro puro
- Es homogéneo, fácil de contar
  - Un Kg de oro siempre es igual a otro Kg de oro (es fungible)
  - Una gallina siempre estará más gorda que otra
- Difícil de falsificar
- Su cantidad no aumenta brúscamente
  - El gobierno no puede generar oro de la nada

También la plata lo cumple, en menor medida

Estos son los criterios para ser buen dinero ¿Los cumple el bitcoin?

# Historia del dinero

1. Dinero real. Mercancía con valor intrínseco, monedas que valían el peso de su metal
2. Dinero representativo. Monedas con metal de escaso valor, pero que representaban cierta cantidad de metal valioso, depositado en el banco. Posteriormente papel (China, siglo VII). Certificado de haber depositado cierta cantidad de metal precioso en el banco. *El banco de España pagará al portador cien pesetas*
3. Dinero fiat (del latín "hágase") [3]. El dinero normal actualmente. De curso legal, válido por decreto. Sin valor intrínseco. Se impone en 1971 con la desaparición del *patrón cambio oro*
4. ¿Criptodivisas?

[3] Cuidado con la palabra *dinero fiduciario*. En ocasiones se refiere al dinero representativo (tengo fe en que me cambiarán este papel por oro), en otras ocasiones se refiere al dinero fiat (tengo fe en esto aunque no equivalga al oro)

En el dinero fiat, los bancos *crean dinero de la nada*, con ciertos límites. *Efecto multiplicador de la reserva fraccionaria*

- Base monetaria
  Reserva de dinero del banco central más dinero en metálico
- Masa monetaria
  Dinero total en el sistema. Dinero en metálico mas depósitos. Solo una parte de este dinero se corresponde con la base monetaria, típicamente el 10 %

De cada 10 EUR que maneja un banco, 9 se los ha *inventado*

El dinero que usamos hoy está respaldado por el estado. Una crítica habitual al bitcoin es *no vale nada porque no lo respalda el estado* Argumento fácilmente rebatible. Los siguientes activos tampoco los respalda el estado

- El oro
- Los diamantes
- Un cheque regalo de El Corte Inglés
- Una ficha del casino de Madrid
- Un piso en la castellana

¿No valen nada?

Dinero es cualquier bien que sirva como

- Medio de pago,
  para el intercambios de bienes y servicios sin los problemas del trueque
- Unidad de cuenta,
  referencia para medir bienes y servicios
- Reserva de valor,
  que conserve poder adquisitivo para ser empleado en el futuro

El respaldo estatal no es una característica esencial. De hecho, el dinero existía mucho antes de que aparecieran los estados

Aquí tenemos otra opinión sobre el bitcoin, mejor informada

- *El dinero no existe, es simple fiducia. Desde la desaparición del patrón cambio oro, las monedas no están respaldadas por nada más que la confianza que depositamos todos en ellas. No hay dinero suficiente, mejor dicho, no vale lo suficiente, para respaldar las operaciones anotadas de todo tipo que teóricamente amparan. Si fuéramos a cualquier banco los depositantes a sacar todo el dinero a la vez, ningún banco nos lo podría dar, porque no lo tiene, porque no existe. Si los tenedores de bonos, letras, pagarés, de cualquier país los vendieran a la vez, ningún país podría pagarlo, iría a la banca rota o al corralito. Si los accionistas de cualquier empresa vendieran todas las acciones a la vez, la empresa más grande quebraría. Así es que, imaginaros el fraude del Bitcoin. O no. Es el fraude del dinero como tal. Bitcoin simplemente lo hace más claro, más visible, más moderno* [4].

[4] Blofeld, elmundo.es, febrero 2014

# Bitcoin

Bitcoin es una *criptodivisa* y un sistema p2p de pago

- Empieza a funcionar en 2009. Autor(es) desconocido(s). Bajo el seudónimo *Satoshi Nakamoto*, desarrolla el protocolo y una implementación completa: *Bitcoin-Qt*
- Proyecto comunitario y de software libre
- Está basado en criptografía, tanto para crear como para gestionar el dinero
- No depende del gobierno de ningún estado. Nadie impone su uso, los individuos son libres para utilizarlo o no
- Se puede intercambiar por dinero fiat, a particulares o a empresas especializadas en cambio de divisas
- Cada vez hay más comercios de todo tipo que lo aceptan como medio de pago, la previsión es que su número aumente exponencialmente

- La masa monetaria y la inflación están prefijadas matemáticamente. Tiene carácter deflacionario a largo plazo. Nadie puede alterarlo, manipularlo, falsificarlo ni producirlo fuera de la forma preestablecida
- Es un sistema distribuido sin autoridad central: será válido lo que la mayoría (simple) de la red considere válido
- Los bitcoins se crean mediante el *minado*, basado en una *prueba de trabajo* (*proof of work*). Consiste en la resolución de cierto problema criptográfico, que exige una elevada capacidad de cálculo

Los terminos en inglés son *bitcoin* y *bitcoins*. En rigor, en español deberíamos decir *bitcóin* y *bitcoines*, aunque quien os habla sospecha que cuando el concepto se popularice, los hispanoparlantes empleramos los términos ingleses

- Los usuarios operan con sus fondos y los almacenan en un software llamado *cliente bitcoin* o *cartera electrónica*
- En rigor el propietario de un bitcoin no es un usuario (o su alias), sino que cada bitcoin o fracción está asociado a un par de claves
  - Una clave pública, de la que se genera la dirección donde se reciben los fondos
  - Una clave privada, que el usuario debe custodiar con mucho cuidado. Si la pierde, habrá perdido irreversiblemente su dinero
  - A partir de la clave privada es sencillo conocer la clave pública asociada. A partir de la clave pública, es imposible conocer la clave privada

  Normalmente los usuarios manejan varios pares de claves

- Los bitcoins son, esencialmente, apuntes contables almacenados en una red p2p
- Participar en la red es gratuito. Realizar transacciones es muy barato o incluso gratuito
- A los usuarios que generan bitcoins mediante minado se les denomina *mineros*. Son quienes mantienen la integridad del histórico de todas las transacciones
  - En opinión de quien os habla, el término *minero* no es muy afortunado. Tal vez la sociedad entendería mejor el bitcoin si a los mineros se les llamase *notarios*, pues ejercen como tales y son retribuidos por ello

# Utilidad del bitcoin (I)

El Bitcoin es útil para operaciones perfectamente legales

- Es un medio de pago conveniente, cómodo y seguro. (A falta de que las herramientas software maduren un poco)
- Permite transferir dinero entre cualquier lugar del mundo de forma casi gratuita y muy rápida. No hay fronteras
- No tiene los riesgos asociados a las tarjetas de crédito (una tarjeta de crédito es muy fácil de clonar fraudulentamente, un pago con bitcoin es imposible)
- Para hacer un pago, basta mostrar un código QR: en un teléfono, en un anuncio, en TV...
- Se evitan los gastos de los operadores tradicionales, como bancos y tarjetas de crédito. En los paises más avanzados las comisiones pueden ser del 3 %, en otras zonas del mundo, estos precios son muy superiores

# Utilidad del bitcoin (II)

- De las tres funciones de una moneda (medio de pago, unidad de cuenta y reserva de valor), probablemente lo primero en extenderse será su utilidad como medio de pago:
  - Los usuarios podrán seguir usando dinero convencional para contabilizar salarios y precios
  - En las transacciones, cuando el dinero se mueva por la red, se *convertirá en bitcoin* sin que el usuario necesite percibirlo
  - Para ello es necesario que haya empresas ofreciendo servicios bancarios. Los bancos tradicionales empiezan a estar interesados y ya están investigando e inviertiendo (Nasdaq, Goldman Sachs, Bankinter, BBVA, ING, UBS, USAA, BNY Mellon, entre otros)
    Los bancos fueron las primeras entidades importantes en informatizarse, siguen utilizando protocolos de los años 50 y 60, antiguos, caros e inseguros y son conscientes de ello

# Utilidad del bitcoin (III)

- Es un medio de almacenar valor que, a diferencia del dinero fiat, no se degrada por la inflación
  - En lugares como Europa o Norteamérica, esto es conveniente
  - En Africa o Latinoamérica, mucho más

  El bitcoin podría llegar a jugar un papel similar al que hoy realizan el oro y los diamantes. Hay quien le llama *oro 2.0*
- Permite micropagos: se puede pagar una cantidad mínima para leer cierta noticia, oir una canción, demostrar apoyo a una iniciativa...
- Los micropagos son aplicables también a los algoritmos de Internet. El modelo actual, donde casi todo es gratis, resulta muy caro porque hay que controlar todo tipo de abusos. Con bitcoin se pueden pagar cantidades minúsculas por los servicios, p.e. millonésimas de euro. Esto es imperceptible para un uso legítimo, pero hace inviable el abuso

# Utilidad del bitcoin (IV)

- Permite el acceso a servicios bancarios a quienes no tienen un banco pero sí un teléfono móvil (cientos de millones de personas, en el primer, segundo y tercer mundo)
- Si se desea, es posible exponer públicamente cómo se ha gastado hasta el último céntimo (útil para ONG, partidos políticos...)
- Si se desea, se puede justificar cualquier pago hecho. De forma no falsificable
- Si se desea, un pago puede ser anónimo (aunque ahora el anonimato no es completo, previsiblemente se conseguirá con mejoras adicionales)
- No depende de la confianza en un banco, empresa o gobierno, sino en el algoritmo

# Utilidad del bitcoin (V)

- Facilita y abarata el intercambio de divisas fiat
- Permite dejar constancia de todo tipo de declaraciones, contratos, transferencias de propiedad, autoría
- Permite operaciones condicionadas: a que se de cierta circunstancia, cierta fecha, que firmen varias personas...
- Las *colored coins* permiten la emisión de *acciones* a cualquier sociedad, sin las barreras de entrada y los costes de los mercados de bolsa tradicionales, que son muy altos

El potencial de estas característica es muy elevado, va más allá de la moneda. Convenientemente desarrollado, podría suponer una revolución en el ámbito financiero

# Utilidad del bitcoin (VI)

El bitcoin permite operaciones ilegales, pero aceptadas por un porcentaje muy significativo de la población: evasión fiscal

- Las operaciones en bitcoin, por su propia naturaleza, son tan incontrolables por los estados como el manejo de dinero en metálico
  - Realmente, más incontrolable. Los evasores no necesitarán mover maletines con billetes a través de las fronteras
- Respecto a *convertir* el dinero fiat en bitcoins o viceversa
  - En la actualidad la manera más habitual es mediante intermediarios financieros, que sí pueden ser controlados por los estados
  - Si se realiza en metálico, es incontrolable
  - Si el bitcoin llega a popularizarse como medio de pago, no será necesario intercambiarlo por dinero fiat

# Utilidad del bitcoin (VII)

Como cualquier dinero, el bitcoin permite operaciones abiertamente delictivas, realizadas por muy pocas personas, pero con muchos recursos. (Tráfico de armas, drogas, blanqueo de dinero, etc)

- Los bitcoins eran una herramienta básica en Silk Road, un mercado online dentro de la red tor que se dedicaba fundamentalmente al comercio de drogas. El FBI lo cerró en octubre de 2013. Tras un periodo de duda, estas monedas fueron subastadas en junio de 2014, lo que supuso un respaldo al bitcoin (si fuera algo ilegal habrían sido destruidas)
- Este fenómeno se ha repetido varias veces en diversos paises

# Situación actual del bitcoin

Actualmente (2015 - comienzos de 2016) destaca:

- El precio se está recuperando respecto a la bajada de 2015 (En 2015 se dieron mínimos por debajo de 200 USD y en la actualidad ha vuelto al entorno de los 380 USD-400 USD )
- Una discusión muy controvertida sobre cómo incrementar la capacidad actual de procesamiento de transacciones de bitcoin (discusión sobre el tamaño del bloque)
- La aparición de fuertes inversiones en todo tipo de iniciativas dentro del ecosistema bitcoin. Muchas provenientes de entidades bancarias tradicionales como Goldman Sachs, Barclays, BBVA, Deutsche Bank o Bankinter
  - Algunas entidades invierten en proyectos basados en bitcoin
  - Otros apuestan por *blockchains* privados. Destaca el consorcio R3.

# R3 CEV's Consortium: 42 Banks with Combined $600bn+ Market Cap; 60% Are Global SIFIs


Source: CoinDesk

State of Bitcoin and Blockchain 2016 CoinDesk 99

# Blockchain pública / blockchain privada

A partir del año 2015 se empieza a hablar de otra variante de la tecnología de bitcoin: las cadenas de bloques privadas, donde solamente pueden participar ciertos organismos autorizados.

- En opinión de muchos especialistas, y de quien os habla, las *blockchain privadas* no tienen sentido, una *blockchain pública* y universal, como bitcoin es más conveniente para cualquier uso
- Las ventajas de bitcoin / blockchain están inseparablemente ligadas a su naturaleza universal, pública y distribuida

- Si un conjunto de entidades financieras quiere intercambiar información, tecnologías tradicionales como las bases de datos y las firmas digitales son mucho más adecuadas
- Una cadena de bloques es una base de datos cara y lenta. Su ventaja radical es que las transacciones son irreversibles con seguridad absoluta. Si la blockchain es privada, sus propietarios pueden modificarla, ya no tiene sentido
- Es cierto que muchos protocolos actuales como SWIFT están anticuados. Pero se pueden modernizar, sin necesidad de cadenas de bloques

- A finales de los años 1990 sucedió algo similar: grandes empresas como Microsoft, Telefónica o America Online intentaron desarrollar copias privadas de internet. Un rotundo fracaso
- A mediados de los años 2000 volvió a suceder: las operadoras de telefonía móvil intentaron desarrollar redes privadas para que los usuarios no tuvieran que acceder a la internet pública desde el móvil. Un rotundo fracaso

- Pero aunque estemos equivocados y las cadenas de bloques privadas tengan éxito, es casi imposiblen que acaben con la cadena de bloques universal (bitcoin)
- Y la diferencia entre bitcoin y otros intentos de hacer cadenas de bloques universales (altcoins) es tan grande, que hace prácticamente imposible que bitcoin sea reemplazado. El *efecto red* es ya muy fuerte
  - Para mejorar la funcionalidad de bitcoin no es necesario sustituirlo, lo natural es añadir nuevas capas de software, como las *sidechains*

# Madurez de bitcoin

Es frecuente oir *Bitcoin ha fracasado, el precio lleva un año bajando y no lo usa nadie*

- Para rebatir esta afirmación, comparemos Bitcoin con Internet
- Internet es una tecnología que ha revolucionado nuestra sociedad en muy poco tiempo. Pero ¿qué significa *poco tiempo*?
- Hoy Bitcoin tiene 7 años. En ese tiempo, en Internet aún no existía Paypal, Terra, Facebook, Youtube...

# Aparición de los principales servicios de internet

- Internet moderna (World Wide Web) 1990
- Lycos 1994
- Amazon 1995
- Altavista 1995
- Yahoo 1995
- eBay 1995
- Hotmail 1996
- ICQ 1996
- Netflix 1997
- PayPal 1998
- Google 1998
- Terra 1999
- Napster 1999
- BitTorrent 2001
- eMule 2002
- WordPress 2003
- Myspace 2003
- Linkedin 2003
- Facebook 2004
- Gmail 2004
- Youtube 2005
- Megaupload 2005
- Twitter 2006
- Spotify 2006
- Airbnb 2008
- Dropbox 2008
- WhatsApp 2009
- Uber 2010

El desarrollo de Bitcoin debería ser más rápido que el de Internet, puesto que

- La inmensa mayoría de la infraestructura necesaria ya está disponible
  - En los años 90 había que comprar un ordenador de 200.000 pts y pagar una tarifa mensual por la conexión
  - Hoy basta instalar una *app*
- Nuestra sociedad ya ha aprendido que una tecnología nueva basada en internet puede cambiar completamente una industria en poco tiempo

Pero tampoco es realista esperar una adopción global instantánea

Recientemente se ha hecho habitual la frase *no nos interesa el bitcoin, sino su tecnología*

- Bitcoin no es solo una moneda o un medio de pago, es un gran libro contable, universal, casi gratuito e inmutable donde cualquiera puede añadir cualquier entrada
  - Nasdaq estudia emplearlo para el control de propiedades en mercados financieros
  - Gobiernos como el británico animan a las empresas a usarlo

Pero si bitcoin alcanza la madurez, estabilidad y legitimidad necesaria para estos usos *secundarios*, se cumplirán todas las condiciones necesarias para su uso *primario* (medio de pago, unidad de cuenta y reserva de valor)

# Bitcoin y economía

- En febrero de 2016 la base monetaria del bitcoin equivale a unos 5600 millones de dólares
- La cotizacción es muy volátil. 0.1$ en 2010, 1$ en 2011, 13$ en 2012, 200$ en 2013, 1000$ en noviembre de 2013, 560$ en marzo de 2014, 685$ en junio de 2014, 166$ en enero de 2015, 375 $ en febrero de 2016...
- La cotización puede consultarse en sitios como bitcoinwisdom.com
- Las súbidas y bajas de precio, como en cualquier divisa, permiten hacer *trading*: comprar o vender con la intención de predecir el precio futuro y obtener una plusvalía
  - Esta actividad puede ser muy lucrativa, pero es muy peligrosa. La inmensa mayoría de los *traders* pierden dinero

Bitcoin no es un esquema de Ponzi (estafa piramidal), porque:

- No hay promesa de beneficio
- La subida no es constante (los altibajos son continuos)
- El bien adquirido no es opaco
- No hay un maquinador central beneficiado por el proceso

Podría tratarse de una burbuja. Ej: burbuja de los tulipanes en Holanda, siglo XVII o la actual burbuja inmobiliara en España

- Aunque una burbuja diferente a las que conocemos
- ¿Qué calidad tiene un tulipán como dinero? ¿Y un piso? ¿Y un bitcoin?

- Actualmente hay unos 12 millones de bitcoins en circulación
- El ritmo de generación de nuevos bitcoins está prefijado por el protocolo
  - Se regula adaptando el nivel de dificultad en el minado
  - Es muy bajo, actualmente unas 150 nuevas unidades por hora
  - Cada vez será más bajo, el ritmo se divide entre dos cada cuatro años
  - Nunca habrá más de 21 millones de unidades en circulación

  La falta de bitcoins nunca será un problema, es una unidad de medida, se puede fraccionar todo lo necesario
  - Un único bitcoin sería suficiente para toda la economía del planeta. Bastaría operar con cifras decimales con muchos ceros después del punto

Si el bitcoin fuera la moneda de un país cuya economía se fortaleciera mucho, la demanda aumentaría. El gobierno del país *imprimiría* más moneda para satisfacer la demanda y regular el precio

- En principio algo similar a Zimbawe, pero legítimo por estar respaldado por una economía fuerte. El valor de la moneda no caería

Pero el ritmo de emisión de bitcoins no depende de la demanda, siempre es el prefijado. Si el uso del bitcoin (la demanda) siguiera aumentando exponencialmente, con una oferta (en comparación) casi constante, el valor (el tipo de cambio frente al fiat) necesariamente deberá seguir aumentando de forma exponencial

- El propósito es favorecer el ahorro. En el caso de quienes compren en las fases iniciales, las plusvalías resultarían espectaculares (como ya lo han sido en el pasado)

# Ecosistema

En torno a bitcoin está surgiendo un gran número de empresas, el llamado *ecosistema*

- casas de cambio (*exchanges*)
- Procesadores de pagos
- Monederos
- Servicios financieros
- Minería
- Desarrollo de software
- Universales (combinan las categorías anteriores)

La inversión de capital riesgo en bitcoin en 2014 fue de 347 millones de dólares.

En el año 2015 se espera que la cifra supere los 1000 millones de dólares

`http://tinyurl.com/ndg4gdp`
`http://tinyurl.com/pcfhhbl`

# Futuro del bitcoin

En opinión (especulativa) de muchos especialistas

- El bitcoin probablemente supondrá una revolución comparable al correo electrónico, el intercambio de música y películas, eBay, las redes sociales o la mensajería gratuita en el móvil
- Cuando esto suceda, su tipo de cambio con el dinero fiat probablemente no sufrirá cambios tan extremos como los actuales. La volatilidad actual es un inconveniente serio para su uso
- Aunque el tipo de cambio se mueva entre rangos no tan variables como los actuales, es imposible saber cuáles serán

Algunas especulaciones (especialmente aventuradas) [5] llegan a decir que el valor del bitcoin en 2017 podría llegar a multiplicar por 1000 el valor en 2014.

- Esto supondría un volumen de tráfico equivalente al 1 % del de Visa
- Este hecho (multiplicar su valor por 1000) ya sucedió entre 2011 y 2014
- Aunque son pocos los que se atreven a dar cifras concretas

[5] http://tinyurl.com/p4xw79f

Si bien podría suceder que los estados implantaran medidas agresivas contra las criptodivisas

- Paises autoritarios como Bangladesh, Ecuador y Bolivia ya lo han hecho
- En paises *occidentales* la regulación que empieza a aparecer se centra en cómo debe contabilizarse, para pagar los impuestos *ordinarios*
  Tal vez en un futuro los estados combatan las criptodivisas con impuestos especiales
- De momento, las autoridades financiaras de paises como Reino Unido, Holanda, Nueva Zelanda, India e Israel han hecho afirmaciones muy favorables a las criptodivisas
- La prohibición de los gobiernos no eliminaría las criptodivisas, de la misma forma que la prohibición no elimina el delito. Pero sería un serio desincentivo

# Bitcoin: riesgos actuales

Muchos de los riesgos asociados al bitcoin se pueden evitar fácilmente aplicando unas poca reglas elementales:

- No dejar los bitcoins en manos de terceros
- Usar software correcto en equipos razonablemente protegidos,
- Custodia adecuada de contraseñas
- etc

Riesgo de tipo de cambio

Posible pérdida que se puede producir por las variaciones de la cotización del bitcoin frente al dinero fiat

- Si compro bitcoins hoy y los vendo el mes que viene, el cambio frente al fiat puede haber variado mucho. Previsiblemente este fenómeno se atenuará con el tiempo
- Si el bitcoin se usa solo como medio de pago en operaciones basadas en fiat, no hay riesgo:
  - Quien envía los fondos, compra una cantidad concreta para una operación concreta y los transfiere inmediatemante
  - El receptor vende los bitcoins, también de forma inmediata
  - El *ecosistema bitcoin* están desarrollando muchas plataformas para facilitar esto

# Bitcoin: riesgos futuros

- Obviamente son imprevisibles: desincentivos estatales, colapso de la minería, aparición de una alternativa mucho mejor... Quien os habla es muy optimista sobre el futuro de bitcoin y atribuye a estos sucesos una probabilidad muy baja
- Puede aparecer un *cisne negro*:
  *suceso de alto impacto, difícil de predecir, fuera de las expectativas normales de la historia, la ciencia, las finanzas y la tecnología*

# Monedas alternativas

A partir del bitcoin, han ido apareciendo otras monedas similares (denominadas *altcoins*):
Ripple, litecoin, peercoin, dodgecoin, pesetacoin y muchas otras, más de 500

`http://coinmarketcap.com/`

- Algunas surgen como intento intentos legítimos de mejorar bitcoin
- Otras son intentos de beneficiarse de un esquema piramidal clásico

El bitcoin es, con mucha diferencia, la criptodivisa mejor situada actualmente. Pero podría perder su posición y dar paso a otra moneda, por diversos motivos, como

- Mejoras técnicas importantes
- El apoyo de una o más grandes empresas (Amazon, Visa, Google, etc)

Esto podría provocar cualquier cosa: desplome, coexistencia, transición brusca, transición suave

# Argumentos a favor de las altcoins

- Bitcoin fue la pionera, pero hay otras criptodivisas presentes con mejoras técnicas muy variadas y muy importantes. Y en el futuro sin duda aparecerán más
- Es muy pretencioso creer que has *acertado a la primera*, Bitcoin podría ser como Napster o MySpace, precursores en su día pero completamente superados hoy
- Diversas criptodivisas pueden coexistir, para distintas finalidades. Aunque el bitcoin sea como el oro, puede haber algo como la plata

# Argumentos en contra de las altcoins (1)

- *Efecto red*: A mayor adopción mayor utilidad, y a mayor utilidad mayor adopción. Lo más importante de una divisa es que inspire confianza, todo lo demás es muy secundario
  - Supongamos dos criptodivisas con implantación similar, una ligeramente por encima de otra. ¿Cuál comprarías? Sin duda, la que esté algo por encima. Todo el mundo hace lo mismo y el efecto se realimenta
  - Pero el caso no es este. La diferencia entre el bitcoin y todas las demás ya es muy elevada, y aumentando
- Actualmente las empresas de capital riesgo están muy interesadas en el *ecosistema bitcoin*, desarrollando todo tipo de plataformas. Ninguna *altcoin* tiene nada similar

# Argumentos en contra de las altcoins (2)

- Cualquier mejora técnica de otras criptodivisas puede incorporarse al bitcoin mediante *side chains*
- Supongamos que aparece una segunda moneda que provoca una pérdida del valor del bitcoin. ¿Alguien confiaría en esta segunda moneda? ¿Para volver a perder cuando se imponga una tercera?
- La plata es útil para transacciones de poco valor, no es práctico usar fracciones muy pequeñas de oro. Pero el bitcoin se puede dividir todo lo necesario

En opinión de quien os habla, los argumentos contra las *altcoins* son mucho más sólidos que los argumentos a favor.

# Side Chains

- El protocolo de bitcoin sirve para almacenar de forma pública y segura el registro de muchos tipos de transacciones entre individuos, no solo de bitcoins. Es aplicable a propiedades inmobiliarias, nombres de dominio...
- Se empieza a hablar de *cadenas laterales (side chains)*: Implementar las funcionalidades de las que carece bitcoin no en criptodivisas nuevas, sino en otras cadenas respaldadas a su vez por la de bitcoin. Análogo a las monedas hasta 1971, que estaban respaldas por oro.
  Bitcoin sería el *TCP/IP* de las nuevas finanzas
- Potencialmente la base de *contratos inteligentes*. Nick Szabo, *The idea of smart contracts*, 1997.
  Propiedad y garantías se gestionen sin autoridad central, solo mediante criptografía, que puede estar integrada en objetos físicos

# Direcciones de bitcoin

Los fondos se almacenan y se transfieren entre direcciones del protocolo bitcoin

Ejemplo: `16ytPRYAJ8D9TikpbnVT9feBEoDur962cg`

- Lo único necesario para un usuario envíe fondos a otro, es conocer esta dirección donde se hará el ingreso
  No hay problema en hacer esta información pública, la dirección es anónima y solo sirve para aceptar bitcoins
- Una dirección está formada por entre 27 y 34 caracteres en Base58
  - Las direcciones incluyen una serie de *hashes* muy robustos que hacen extremadamente difícil que una dirección construida (o modificada) al azar sea válida. Esto impide que alguien pueda enviar fondos a una dirección equivocada
  - Base58 es una codificación alfanumérica que evita ciertos caracteres que pueden resultar ambiguos para las personas: `0,O,l,I,+,/` (cero, o máyuscula, ele minúscula, i mayúscula)
    Es sensible a mayúsculas

# Claves privadas

Cada dirección tiene una clave privada asociada, formada por 32 bytes. Quien conozca esta clave, y solo quien conozca la clave, controla el saldo asociado

Formas de representar la clave

- Hexadecimal, p.e.
  `E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4`
  `45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62`

- *Wallet import format*. Es la manera más habitual, 51 o 52 caracteres en base58. p.e.
  `5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF`

- *Mini private key format*
  30 caracteres en base58. Especialmente útil para generar códigos QR. No cualquier clave privada puede representarse así, es necesario crearla con este propósito. p.e.
  `SzavMBLoXU6kDrqtUVmffv`

# Símbolo y fracciones

- Actualmente lo más habitual es emplear la abreviatura BTC para indicar bitcoin. En 2013, la norma ISO4217 le asignó el código XBT.
  - La X inicial se usa para activos que no son monedas oficiales, como el oro (XAU) o la plata (XAG)
- 1 BTC = 1 bitcoin
  0.01 BTC = 1 cBTC = 1 centibitcoin, *aka* bitcent
  0.001 BTC = 1 mBTC = 1 milibitcoin *aka* mbit
  0.000 001 BTC = 1 $\mu$µBTC = 1 microbitcoin, aka ubit
  0.000 000 01 BTC = 1 satoshi
- Se está considerando emplear fracciones más amistosas para el usuario, como el *bit* (una millonésima de bitcoin)

# Tiempo de las transacciones

En principio, para estar completamente seguro de que la transacción se ha realizado correctamente, se considera que hay que esperar a que conste en 6 bloques (6 confirmaciones), lo que puede tardar unos 25 minutos

- En la práctica, para cantidades no muy elevadas con 2 o 3 confirmaciones es más que suficiente
- Mediante técnicas adicionales, como el uso de procesadores de pago, la operación es instantánea
  - Entre otras cosas, el procesador comprueba que la transacción figura en varios nodos diferentes por toda la red, por eso le basta con 0 confirmaciones

# Protocolo de bitcoin: idea básica

El protocolo de bitcoin tiene cierta complejidad, veremos aquí una metáfora que busca ser didáctica, no rigurosa
Supongamos un grupo de personas juega al póquer y no quiere usar fichas físicas. Tienen 3 fichas virtuales. Confían en una persona con autoridad, que apunta las transacciones en una pizarra a la vista de todos

```
Sandunguero74 posee la ficha 1 y la ficha 2
AmebaLaboriosa posee la ficha 3
Sandunguero74 le da la ficha 1 a Replicante
```

Así funciona el dinero fiat. Nuestras nóminas, transferencias y cargos en la tarjeta de crédito solo son apuntes contables. No en un único registro (un único banco) sino en varios, pero todos coordinados bajo la autoridad del estado

Supongamos que los jugadores no quieren depender de un único operador de la pizarra. Así que cada transacción la notifican en voz alta a toda la mesa, y cada uno va apuntando en su propia pizarra todas las transacciones, todos mantienen una copia igual
Cada pizarra incluye una pequeña cabecera con los datos de cada jugador

```
Pizarra de Sandunguero74                    <--------- (Cabecera)
------------------------
Sandunguero74 posee la ficha 1 y la ficha 2
AmebaLaboriosa posee la ficha 3
Sandunguero74 le da la ficha 1 a Replicante


Pizarra de AmebaLaboriosa
-------------------------
Sandunguero74 posee la ficha 1 y la ficha 2
AmebaLaboriosa posee la ficha 3
Sandunguero74 le da la ficha 1 a Replicante


Pizarra de Replicante
---------------------
Sandunguero74... etc etc
```

- Al cabo de unas cuantas operaciones, todas las pizarras se habrán llenado. En este momento, la sala tiene que decidir que una sola de las pizarras será la definitiva: transferida a papel, encuadernada y aceptada como oficial por todos para siempre
- Todos los participantes compiten entre sí para conseguir que su pizarra sea la definitiva, porque quien lo consiga recibirá un par de fichas como premio.

Lo primero será contrastar cada pizarra con todas las pizarras desde el principio de los tiempos, para comprobar que cada ficha haya sido creada correctamente y que no sea gastada dos veces

```
Pizarra de AmebaLaboriosa
-------------------------
Sandunguero74 posee la ficha 1 y la ficha 2
AmebaLaboriosa posee la ficha 3
Tramposillo entrega la ficha 4 a Replicante     <---------
Sandunguero74 entrega la ficha 1 a Replicante
Tramposillo entrega la ficha 4 a Sandunguero74  <---------
```

Una vez limpiadas las transacciones incorrectas, cada jugar intenta resolver una especie de sudoku con los datos de su pizarra tentativa para convertirla en la pizarra definitiva.
Tiene que añadir a su pizarra un valor (llamado nonce), de forma que cuando se aplique al conjunto el doble hash SHA-256, el resultado sea un número que empiece por 4 ceros seguidos.
Por tanto, cada pizarra tentativa contendrá:

- La cabecera, que será distinta para cada jugador
- Las transacciones correctas, que serán iguales para todos
- Un nonce, el valor que intenta encontrar cada jugador

La búsqueda del nonce sería algo parecido a esto:
Replicante toma la cabecera, las transacciones y prueba el nonce jh00. Calcula el hash SHA256, y al resultado, le vuelve a calcular el SHA256

```
replicante@spinner:~$ echo "Pizarra de Replicante , jh00 , Sandunguero74
entrega la ficha...." |sha256sum |sha256sum
1941bd6309c21d6c9c6b52069b612ae5664dd932536446390 40ffd80b4049df7
```

Pero le sale un hash que empieza por 1941, no vale

Ahora prueba con el nonce jh01

```
replicante@spinner:~$ echo "Pizarra de Replicante , jh01 , Sandunguero74
entrega la ficha...." |sha256sum |sha256sum
9f752a664adac484460d87f45ad1aac809b1abc78388edbc25a7760244f88d46
```

El hash obtenido empieza por 9f75, tampoco vale

- Obsérvese que un cambio de un solo bit en la pizarra tentativa (el cambio del nonce) genera un hash completamente distinto. La única forma de buscar el nonce es la fuerza bruta, ir tanteando valores secuencialmente

Tras muchos cálculos, AmebaLaboriosa ha encontrado un nonce, xb84, que encaja en su pizarra y que resuelve el problema

```
replicante@spinner:~$ echo "Pizarra de AmebaLaboriosa , xb84 , Sandungu
entrega la ficha...." |sha256sum |sha256sum
00001b50e2ade721b07e191ff72773ec87736883d9ad63593080f00ef83ce84b
```

En realidad las transacciones de esta pizarra no son iguales a las de todas las demás: AmebaLaboriosa había tenido la precaución de añadir una transacción, la creación de las dos nuevas fichas del premio, que ahora le pertenecen

AmebaLaboriosa transmite el bloque a todos los demás, que comprueban que todo es correcto. Averiguar el nonce es muy difícil, comprobar que es válido, es muy fácil

- Todos los participantes reconocen las nuevas fichas como auténticas y pertenecientes a AmebaLaboriosa.
- En la pizarra de Replicante dice que el premio es de Replicante, pero como no ha llegado a ganarlo, esa pizarra se descarta
- La pizarra de AmebaLaboriosa se considera *oficial* y definitiva, se pasa a papel y se encuaderna sólidamente a las anteriores
  Esto es: el bloque se añade a la cadena de bloques

# Protocolo de bitcoin: otros aspectos

Hagamos el modelo un poco más realista:

- Las transacciones se hacen con fracciones de bitcoin, hasta 8 decimales si se desea

  `Replicante envía 0.005 BTC de la ficha 2 a Sandunguero74`

- Cada transacción va firmada con la clave privada de la cuenta origen e incluye la dirección pública de la cuenta destino
- En la red hay dos tipos de usuarios
  - Usuarios ordinarios, que se limitan a hacer transferencias
  - Mineros, que mantienen la cadena de bloques

- En las transacciones no van *nicknames* de usuarios, sino claves públicas. Quien conozca la clave privada asociada, podrá manejar ese bitcoin. Si, por ejemplo, la clave privada se guarda únicamente en un disco duro que *muere* bañado en café, ese bitcoin se ha perdido para siempre
  No hay ningún mecanismo de revocación de claves ni nada similar
- Las transacciones de los bloques tentativos no son válidas, solo tienen efecto cuando el bloque se añade a la cadena. Esto lleva unos 10 minutos. Para confirmar una transacción con certeza absoluta es necesario esperar unos 6 bloques, unos 60 minutos
  - En la práctica este tiempo se puede reducir o incluso eliminar por completo, con la ayuda de herramientas adicionales

- Cada bloque lleva el hash del bloque anterior, esto forma una cadena con todas las transacciones de la historia, cuya integridad está garantizada criptográficamente
- En la actualidad cada bloque creado tiene un premio de 25 BTC. Está previsto que el premio se vaya reduciendo con el tiempo, hasta alcanzar una masa monetaria de 21 millones de bitcoins en el año 2140
  Eso no significa que el protocolo *caduque*
  - En ese momento se podrían añadir más decimales a las operaciones, si fuera preciso
  - La retribución de los mineros vendrían por el pago por las transacciones

# Los mineros

- Originalmente, el software del cliente podía minar, pero al poco tiempo se separaron las funciones de usuario ordinario y de minero
- Cualquiera que lo desee puede ser minero
- No importa si hay mineros maliciosos, con tal de que la mayoría (simple) de la red sea honesta
  - Un conjunto de mineros maliciosos podrían intentar crear una ramificación propia de la cadena, pero nadie la usaría porque la cadena legítima sería más larga
- Los mineros se asocian en grandes *pools* , existe el riesgo de que un *pool* supere el 51 % del total
  GHash consiguió esto durante unas horas en junio de 2014, disparando todas las alarmas
  Esto es un problema, pero no fatal. Y tiene soluciones

# Dificultad del minado

- Los mineros cada vez tienen mejores ordenadores (ley de Moore), si la dificultad fuera constante, acabarían ganando bitcoins muy rápidamente. Por tanto, el protocolo incrementa periódicamente la dificultad del minado. (Aumenta el número de ceros a la izquierda que se exigen como resultado del doble hash)
  Esto permite que al bitcoin no le pase lo mismo que al dólar de Zimbawe
- Excepto en los primeros tiempos, la rentabilidad de la minería siempre ha sido baja. El nivel de dificultad se adapta para que los mineros cubran gastos y poco más. En paises donde la energía es tan cara como en España, es prácticamente imposible ganar dinero con la minería
- Actualmente los mineros trabajan asociados y con superordenadores

Los usuarios envían las transaccions por broadcast a todos los mineros. Tal vez el minero que genere el bloque ganador no haya recibido alguna transacción en concreto. Esto no tiene mucha importancia, la transacción acabará apareciendo en algún bloque

- Por tanto, un bloque se considera correcto si todas sus transacciones son correctas. No importa si faltan transacciones
- Si una transacción aparece en un bloque tentativo pero no aparece en el bloque definitivo, la transacción es nula. Por eso es muy importante esperar a que las transacciones se confirmen

# Precio de las transacciones

Normalmente las trasacciones no son gratuitas, quien envía los fondos ofrece un pequeño pago al minero, por el importe que desee. Si al minero le parece insuficiente, ignorará la transacción. Valores típicos son 0.1mBTC o 0.2mBTC

- Si el pago que ofrece la transacción es muy bajo o nulo, probablemente acabará entrando en la cadena cuando llegue a algún minero que acepte estas condiciones. Por tanto, pagar más o menos hará la transacción más o menos rápida, pero el protocolo garantiza la integridad del sistema
- Para evitar abusos, algunas transacciones exigen una comisión mínima de 0.1 mBTC: Las que tengan un importe inferior a 10 mBTC, las referidas a bitcoins muy recientes y las muy voluminosas.

# Hash rate y n/confirmaciones

Se define *hash rate* como la potencia de cálculo de todos los mineros de la red
Supongamos que un conjunto malicioso de mineros acordara, en su propio beneficio, aceptar transacciones irregulares

- Generaría una ramificación de la cadena, una subcadena que solamente ellos daría por buena, solamente ellos encadenarían aquí nuevos bloques
- Como tienen menos *hash rate* que la mayoría honesta, serían incapaces de generar bloques al mismo ritmo, su subcadena acabaría siendo más corta que la subcadena legítima

- Pero en un principio, los mineros maliciosos podrían tener suerte y generar bloques a ritmo similar o incluso superior al resto
- Solamente al cabo de n bloques (de n/confirmaciones) se verá cláramente qué cadena es más larga, esto es, cuál ha sido generada por una comunidad de mayor *hash rate*
- Cada cliente decide qué valor de n considera razonable. Para las transacciones, un valor habitual es $n = 6$. Para los nuevos bitcoins, $n = 120$

# Tipos de cartera

La cartera (*wallet*) es el software que gestiona las claves, y por tanto los fondos

Hay varios tipos de cartera

- Carteras *online*
- Carteras locales

  A su vez, estas pueden ser
  - Carteras tradicionales
  - Carteras *frías*
  - Carteras ligeras
  - Carteras ligeras con semilla

# Carteras tradicionales

El cliente original, Bitcoin-Qt fue desarrollado por el propio *Satoshi Nakamoto*. Es la referencia para todos los demás y el único que cumple completamente el protocolo

- Cada cartera almacena localmente las claves privadas de los bitcoins que controla. Típicamente en su disco duro
- Cada cartera (cada cliente) también necesita tener almacenada la cadena completa de transacciones
  Se trata de un fichero de cierto tamaño (del orden de gigas en 2014), pero manejable por un ordenador convencional

# Carteras frías

Las claves privadas (o lo que es lo mismo, los bitcoins) pueden guardarse en carteras *offline*, también llamadas *carteras frias*

- Consiste en almacenar las claves en cualquier medio no conectado a la red
- Se pueden emplear ordenadores sin conexión a internet, soportes digitales (p.e. cdrom), impresión en papel o grabación en metal
  - Es posible generar verdaderos billetes o acuñar monedas
- Además de almacenar los fondos, alguna carteras permiten firmar transacciones offline
- Así, la seguridad de los fondos no depende de nuestra habilidad manteniendo seguro un fichero, sino un objeto físico. Por ejemplo, guardando un cdrom o unos billetes en una caja fuerte de nuestra confianza

Para operar con billetes:

- Se pueden generar los billetes con clientes bitcoin avanzado como *Armory*
  Normalmente usan códigos QR
- Para operar con los fondos, se escanea el billete con cualquier monedero para móvil o tableta y se transfiere la clave a una cartera *online*
- Para robar los fondos, basta pasar un escáner

# Seguridad de las carteras frías

- Solo son seguros los billetes que hayamos impreso nosotros, en otro caso tenemos que confiar que quien lo ha impreso no ha guardado una copia
- Para que la seguridad sea total, también deberíamos custodiar la impresora y jamás deberíamos conectarla a un ordenador conectado a internet, por la posibilidad (remota) de que la impresora o su driver estén comprometidos
- Hay monedas acuñadas, que no son más que impresiones de las claves sobre metal. Quien las acuña siempre promete que no ha guardado las claves, pero de nuevo, tenemos que creer esto. Las monedas no son realmente prácticas, son objetos de colección o de adorno.

# Las carteras online. Ventajas

En este tipo de carteras, un servidor se encarga de la gestión de la cadena de transacciones, así como de la custodia de las claves públicas y privadas del usuario en la red bitcoin

- El usuario accede al servidor, normalmente desde una página web
- La más popular es *coinbase*, que también actúa como *exchange*

Ventajas de las carteras *online*:

- El usuario no necesita almacenar la cadena completa en cada ordenador donde opera
- Si el usuario olvida la contraseña de su cuenta en el servidor, el servidor puede ayudarle a recuperarla

# Inconvenientes de las carteras online

- Debemos confiar en la honestidad el servidor
- Debemos confiar en que su software esté bien hecho
- Estos sitios web almacenan enormes cantidades de bitcoins, son un objetivo muy atractivo para todo tipo de atacantes

La práctica totalidad de incidentes graves de seguridad se han producido en *exchanges* y carteras web

- Multitud de robos: en *mybitcoin*, *bitomat*, *bitcoinica*...
- Cierre de GBL en noviembre de 2013
- Cierre de MtGox en febrero de 2014

Esto se parece mucho al robo en bancos tradicionales, la diferencia es que los bancos cuentan con seguros que protegen a los usuarios y estas entidades no (actualmente no, aunque empiezan a aparecer iniciativas en esta línea)

# Carteras ligeras

La aparición de carteras (locales) ligeras supuso un gran avance de seguridad, pues eliminan los riesgos de carteras *online* sin necesidad de almacenar la cadena completa de transacciones

- Usan una red de servidores que almacenan la cadena
- Las claves privadas se guardan localmente, en el ordenador de cada usuario

# Inconvenientes de las carteras ligeras

- Como todas las carteras locales, si el usuario pierde el fichero que contiene las contraseñas privadas (y no tiene copia de seguridad), pierde su dinero sin remedio
- Teóricamente son vulnerables a ciertos ataques *man in the middle*, pero quien os habla no ha encontrado ningún caso
  - Para minimizar este riesgo, se puede evitar el acceso a internet desde provedores dudosos, como cibercafés y similares

# Carteras con semilla

Las carteras con semilla son un tipo de carteras ligeras donde las claves se generan con un algoritmo pseudoaletorio. Conociendo su semilla, se pueden regenerar todas las claves

- La cartera *electrum* emplea una semilla que representa como una lista de 12 palabras inglesas, por ejemplo
  *pain apologize tired bar change thin off outide clear fear hit stirr*
- Es más sencillo mantener segura esta lista de palabras que una clave de 32 bytes para cada una de nuestras direcciones
- A partir de esta semilla, se pueden generar todas las claves públicas y privadas que se deseen
- Por tanto, el dinero del usuario permanecerá razonablemente seguro mientras esta semilla se mantenga segura

# Compra venta de bitcoins

¿Cómo comprar bitcoins? ¿Cómo convertirlos en dinero fiat?

- Lo más sencillo es conocer a una persona de cierta confianza que quiera comprar o vender: simplemente intercambiaremos el dinero fiat por cualquier medio tradicional y haremos la transferencia de bitcoins mediante nuestras carteras
- Hay algunos establecimientos financieros tradicionales que ofrecen este servicio, aunque actualmente son muy pocos y muy caros
- En algunos países hay cajeros automáticos (muy pocos)
- Lo más habitual es realizar el intercambio en un *exchange*. O en plataformas como `localbitcoins`

# Exchanges

Un *exchange* (casa de cambio) funciona como cualquier mercado de divisas

- Compradores y vendedores (*traders*) presentan sus ofertas de compra (*bids*) y demandas de venta (*asks*)
- Las operaciones son rápidas y anónimas
- El *exchange* tiene el control de toda la operación, en él confian los traders. Es un punto único de fallo

Algunos exchanges donde podemos comprar bitcoins

- Coinbase
- Circle.com
- Bitstamp
- Kraken
- Muchos otros: BTC-e, Safello,

Todos estos organismos están sujetos a las leyes anti blanqueo de dinero, nos exigirán una copia del DNI y acreditar nuestra dirección de residencia (mediante factura de luz, gas, extracto bancario o similar)

# Localbitcoins

`localbitcoins.com` es una plataforma similar a un exchange, aunque con ciertas peculiaridades. Puede ser una buena forma de comprar los primeros bitcoins, aunque resultará un poco más caro

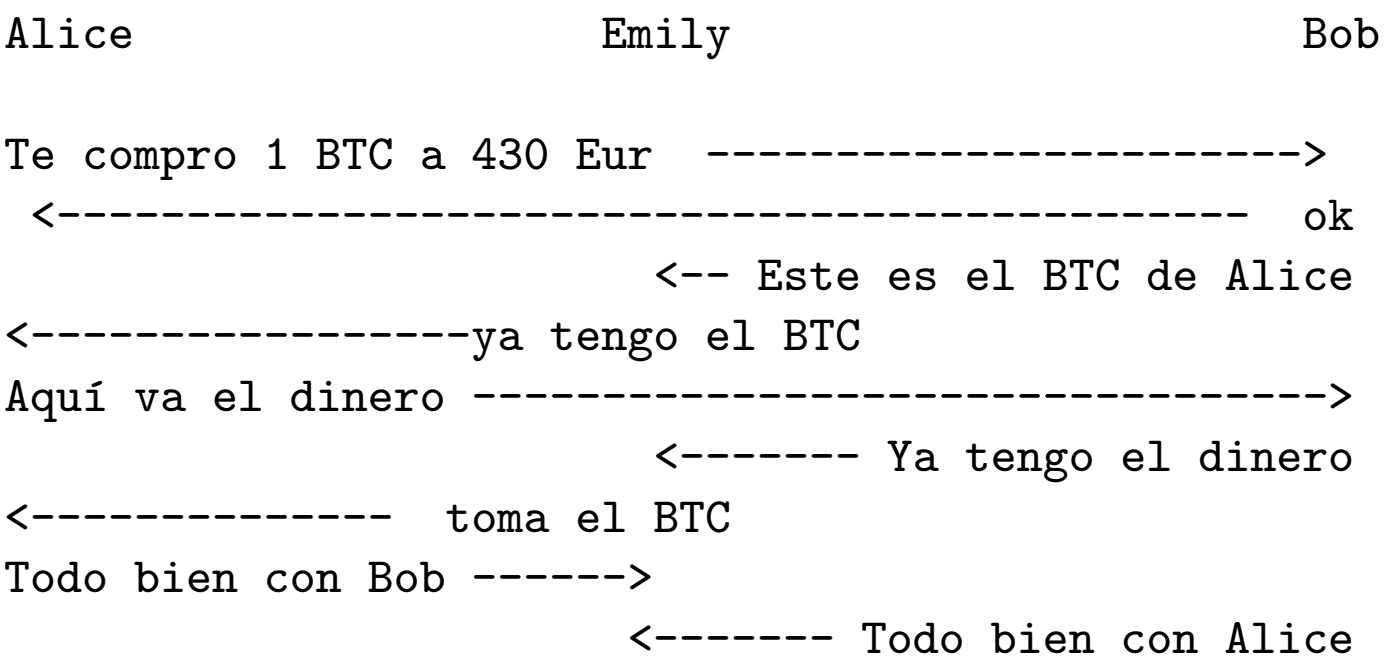
- Es un sitio web donde los usuarios pueden poner sus anuncios ofreciendo la compra o venta de bitcoins. Es un mercado donde cada usuario fija sus propias condiciones, sus propio precio y sus propios límites.
- El sistema gestiona la reputación de los usuarios, cada vez que alguien realiza una transacción, otorga una calificación al usuario con el que ha tratado. El mismo principio que usa eBay
- Ejercer un fideicomiso (*escrow*)
- En caso de conflicto entre partes, realiza una intermediación

# El fideicomiso

Supongamos que Alice quiere comprar bitcoins, y Bob quiere vender. No se conocen entre sí

- Si Alice envía primero su dinero fiat, corre el riesgo de que Bob no le envíe los bitcoins
- Si Bob envía primero los bitcoins, corre el riesgo de que Alice no le envíe el fiat

La solución es contratar a un tercero en quien ambos confían (Emily) para contratar un fideicomiso (*escrow*)
Bob (depositante aka fideicomitente) entrega a Emily (depositario aka fiduciario) los bitcoins para que se los entregue al beneficiario (Alice) siempre y cuando se cumplan ciertas condiciones (la recepción del pago)


Alice
Emily
Bob
Te compro 1 BTC a 430 Eur
ok
<-- Este es el BTC de Alice
ya tengo el BTC
Aquí va el dinero
Ya tengo el dinero
toma el BTC
Todo bien con Bob
Todo bien con Alice

- Alice y Bob probablemente se conocieron por un anuncio en el web de Emily
- Alice y Bob acuerdan libremente el precio
- Emily cobra una comisión por su servicio, por ejemplo el 1 %
- Normalmente, Emily no envía los bitcoins a la cartera local de Alice, sino a una cartera online gestionado por la propia Emily.
  - Lo más recomendable es que Alice transfiera inmediatamente sus fondos a su cartera local. Esto tardará unos minutos, durante los cuales Alice está expuesta a los problemas de las cartera online
    Si precisamente en este tiempo Emily quiebra, o sufre un robo o se comporta fraudulentamente, Alice habrá perdido su dinero sin remedio

# Maleabilidad de las transacciones

Las carteras locales destinadas al usuario final son razonablemente seguras, pero los *exchanges* y las carteras *online* operan con su propio software. En ocasiones han incurrido en fallos de seguridad que han sido atacados

- En el protocolo de bitcoin, la información principal de cada transacción (importe y destino) está bien protegida mediante un hash. Pero algunos campos, no esenciales, no están protegidos
- Se ha descubierto cómo modificar el identificador de transacciones recientes, autorizadas pero no confirmadas
  - Los clientes bien hechos no tomarán decisiones sobre transacciones no confirmadas, pero algunos clientes, como el de MtGox, actuaban imprudentemente

Supongamos que Mallory quiere estafar a Alice

- Alice envía dinero a Mallory, notificando la transacción a la red

  `Transacción 23: Alice envía a Mallory el bitcoin 5`

- Mallory envía a la red una transacción con los mismos datos fundamentales, pero con un identificador distinto

  `Transacción 223: Alice envía a Mallory el bitcoin 5`

  (El identificador de la transacción, 23 o 223, no está protegido por el hash)
- Mallory (que también es minero), consigue que la transacción 223 entre antes en un bloque
- Cuando la transacción 23 llega a la red, es rechazada porque el bitcoin 5 ya no es de Alice
- La transacción 223 se procesa correctamente, es válida porque sus datos fundamentales lo son. El identificador no es relevante

Mallory dice: *Alice, la transacción 23 ha fallado*

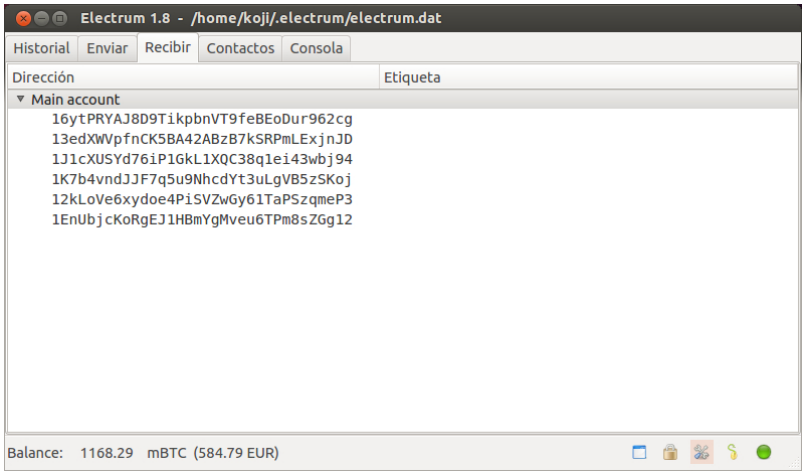
- Si Alice es torpe, responderá
  *Vaya, es cierto, perdona, ahora mismo te vuelvo a enviar el dinero*

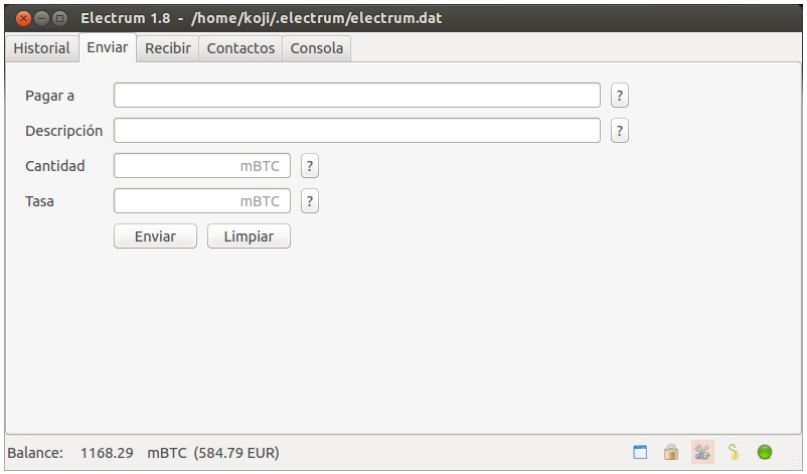
  `Transacción 24: Alice envía a Mallory el bitcoin 72`

  (Obsérvese que hace una transacción nueva, por el mismo importe, pero de un bitcoin distinto)
  Mallory ha conseguido dos bitcoins, los de las transacciones 223 y 24
- Si Alice sabe trabajar bien, responderá
  *Espera media hora*
  Y si pasado ese tiempo Mallory insiste, Alice dirá
  *Ya no tengo el bitcoin, la transacción se ha realizado aunque veo que alguien, probablemente tú, le ha cambiado el identificador, so delincuente*

# Electrum

- Los usuarios avanzados suelen emplear la cartera *Armory*
- En Android se puede usar blockchain, kncwallet y muchos otros
- En esta asignatura usaremos Electrum, una cartera muy sencilla, gratuita y libre disponible para Windows, Linux, Mac y Android.
- Genera todas las claves a partir de una semilla de 12 palabras en inglés



# Uso de Electrum

El funcionamiento de las pestañas *enviar* y *recibir* resulta obvio
Algunas otras opciones útiles:

- Para que la cartera nos muestre una estimación del contravalor de nuestros bitcoins en EUR
  - Linux:

    `File | Ajustes | Visualización | Moneda`

  - Windows:

    `Herramientas | Complementos | Exchange Rates | Ajustes`

- Para que la cartera trabaje siempre en milibitcoins (mBTC)

  `File | Ajustes | Cartera | Base unit`

Electrum guarda la cartera en

- Linux

  `~/.electrum/wallets/default_wallet`

- Windows

  `c:\Users\MINOMBRE\AppData\Roaming\Electrum\wallets\default_wallet`

Si este fichero se destruye no supone ningún problema porque puede ser regenerado fácilmente a partir de la semilla

- Como hemos visto, una semilla tiene este aspecto: *pain apologize tired bar change thin off outide clear fear hit stirr*

Para proteger el fichero `electrum.dat`, Electrum ofrece la posibilidad de cifrarlo con una contraseña (una clave simétrica)

- Para enviar fondos o acceder a la clave privada (de cada dirección de bitcoin), Electrum nos solicitará la contraseña
- Si un atacante robara el fichero `electrum.dat`, no le serviría de nada sin la contraseña
- Metáfora: la contraseña sería la llave del armario donde guardo las llaves (las claves privadas de la red bitcoin)
- Obviamente, el olvido de la contraseña no es un problema, las claves privadas se regeneran fácilmente a partir de la semilla

Por tanto, conocer la lista de palabras de la semilla, permite conocer las claves públicas y privadas de la red bitcoin

- Si un atacante me roba esta lista de palabras, habré perdido mi dinero
- Si olvido esta lista de palabras...
  - Pero conservo las claves privadas, con su contraseña si se la puse, conservo el control de los fondos
  - Y también pierdo las claves privadas o su contraseña, habré perdido mi dinero

En resumen, para manejar Electrum debo distinguir:

- La semilla de 12 palabras que genera las claves públicas y privadas asociadas a cada dirección
- Las claves públicas (aka direcciones) y privadas del protocolo bitcoin, que se almacenan en el fichero `electrum.dat`
- La contraseña con la que, opcionalmente, puedo proteger las claves privadas

# Uso distribuido de Electrum

- Con carteras cuyas claves no estén generadas desde semilla, si quiero trabajar con varios ordenadores, tengo que copiar a todos ellos las claves públicas y privadas
- Con Electrum, basta con usar la misma semilla una vez en cada ordenador
- Obviamente, no hay que hacer nada para mantener el saldo coordinado entre todos los monederos, puesto que el dinero no está en el monedero sino en los registros de la cadena de bloques

En Electrum se pueden importar e usar pares de claves generadas en otros monederos, pero esas claves ya no se generan a partir de la semilla, por tanto

- Hay hay que sincronizar manualmente el fichero `~/.electrum/electrum.dat`
- Hay que custodiar este fichero con el mismo cuidado que la semilla

Lo más recomendable es mover el saldo de la dirección antigua a una dirección generada por Electrum. Aunque si alguien hiciera una transferencia a la dirección antigua, necesitamos conservar la clave privada antigua

# Secret sharing

Aunque pongamos cuidado extremo en guardar nuestra contraseña, esto puede no ser suficiente.

- ¿Y si a pesar de todo, la perdemos o nos la roban?
- ¿Y si no estamos disponibles? (Viaje, enfermedad, muerte...)
- ¿Y si nos secuestran?
- ¿Y si hacemos algún disparate?

Podríamos dividir la contraseña en n trozos y repartirlos entre n personas de nuestra confianza, de forma que con el acuerdo de todos, el secreto es recuperable

- Problema: Bastaría con que se pierda un trozo para perder el secreto
- Solución: Algoritmos de *secret sharing*

Un esquema *secret sharing* es aquel que permite dividir un secreto en n fragmentos, de forma que basten t ($t < n$) para reconstruirlo
Armory incluye esto de manera nativa, con electrum podemos usar una herramienta independiente, ssss
Con la orden `ssss-split`, dividimos el secreto en n fragmentos

```
koji@mazinger:~$ ssss-split -t 3 -n 5
WARNING: couldn't get memory lock (ENOMEM, try to adjust RLIMIT_MEMLOCK
Generating shares using a (3,5) scheme with dynamic security level.
Enter the secret, at most 128 ASCII characters
ABRETE SESAMO
1-378a29cbbe9b38f0d473bdab0654
2-d7cc58bbce72070afc675f0991dd
3-d42a4e6f0dca1d32a6d1f96e4e92
4-629dd862cb052f8774bdb26d91df
5-617bceb608bd35bf2e0b140a4e82
```

Con la orden `ssss-combine`, recuperamos el secreto

```
koji@mazinger:~$ ssss-combine -t 3
WARNING: couldn't get memory lock (ENOMEM, try to adjust RLIMIT_MEMLOCK
Enter 3 shares separated by newlines:
Share [1/3]: 2-d7cc58bbce72070afc675f0991dd
Share [2/3]: 3-d42a4e6f0dca1d32a6d1f96e4e92
Share [3/3]: 5-617bceb608bd35bf2e0b140a4e82
Resulting secret: ABRETE SESAMO
```

Si el secreto es mayor de 128 bytes, se cifra con una clave tradicional y se aplica ssss a esta nueva clave

# Referencias


- *Bitcoin: A peer-to-Peer Electronic Cash System*. Satoshi Nakamoto. `https://bitcoin.org/bitcoin.pdf`
- `http://en.bitcoin.it`
- Wikipedia
- `http://elbitcoin.org`
- `http://blockchain.info`
- http://www.coindesk.com/state-of-bitcoin-blockchain-2016
- twitter: `@MiguelOrtunoP`