Manual de finanzas

Carlos E. Tafur Egido

22/07/2017

Índice general

1 Introducción **1**

2 Vivienda **2**

3 Cuentas bancarias **2**
3.1 Bancos online 2
3.2 Tarjetas 3
3.3 Cuenta Zero 3

4 Tecnologías de criptoactivos **4**
4.1 Blockchain 4
4.1.1 Problemas de los blockchains 6
4.1.2 Bitcoin 7
4.1.3 Ethereum 8
4.2 Hashgraph 11
4.2.1 Stellar 11
4.3 Gestión 12
4.3.1 Wallet 12

1 Introducción

Este documento tiene información sobre la gestión personal de mis finanzas.

2 Vivienda

Encontré un artículo muy bueno sobre si es un mito realmente eso de "Alquilar es tirar el dinero". De todos modos, es difícil. Cada caso es distinto. Me gustaría hacer aquí una lista con las cosas a favor de la compra y a favor de alquilar. TKTKTKTKTKTKTKTKTK.

3 Cuentas bancarias

3.1 Bancos online

Estuve interesado por algunos de los nuevos bancos online que están surgiendo últimamente, como, por ejemplo, Monzo, N26 y Revolut. Por lo que veo, la principal ventaja que tienen respecto a los bancos más tradicionales es que cobran muy poco por los pagos en el extranjero con otras divisas, o incluso llega a ser gratis (por ejemplo, N26 usa el servicio de TransferWise para transferencias con cambio de divisa). También es bastante baja la comisión por sacar dinero en cajeros en otros países. Aparte de eso, tampoco parecen ofrecer mucho más.

Si no estoy equivocado, estos tres bancos proporcionan tarjetas de débito MasterCard. Respecto a la compatibilidad de pagos por NFC, Monzo es compatible con Google Pay, N26, con Apple Pay y Revolut no sé.

Monzo es de Reino Unido, N26, de Alemania y Revolut, no sé. El caso es que, ahora con el Brexit, quizás convendría más que me pasara, en caso de pasarme, a N26.

Lo que sí parece es que la aplicación es algo (aunque tampoco mucho) mejor que en los bancos tradicionales. Suelen hacer una clasificación de forma automática del tipo de gasto; por ejemplo, *gimnasio*, *alimentos* etc. En N26, además, puedes ponerles etiquetas (los llaman *hashtags*; son como los de Twitter) a los gastos, si deseas mayor detalle. Esto también se puede hacer si usas la aplicación Fintonic y la asocias a tu vienta bancaria, por ejemplo, sirve para clientes del Banco Santander.

N26 también permite exportar, como un archivo CSV, el historial de tus transacciones, para así no perderlo si te cambias de banco.

Otra cosa buena que tiene N26 es que los servicios de chat y de asistencia por teléfono los proporciona también en español, además de otros idiomas. Se supone que estos bancos no solo eliminan al empleado en las operaciones básicas, sino Que las operaciones algo más complicadas, como, por ejemplo, pedir un préstamo o una hipoteca, se harán en varias fases, gran parte de ellas mediante un chat que empleará para comunicarse con el empleado.

Algo que no me convence son las condiciones de la tarjeta de N26. Respecto a la retirada de efectivo de los cajeros automáticos, ponen un límite, que puede ser en la cantidad de dinero que puede retirar al mes o el número de veces que puede realizar una retirada. Tampoco me parece un gran inconveniente. El banco que más me convence de estos nuevos es N26, pero el problema que le veo es que no tiene seguro contra robos y estafas. Con la Cuenta Zero del Banco Santander sí los tengo. Actualmente, este es el único inconveniente que le veo y la razón por la que aún no me he pasado a N26.

También estuve viendo otros bancos online españoles, como el OpenBank, que es también (al igual que el Banco Santander) del Grupo Santander. Creo que las condiciones son un poco peor que para la Cuenta Zero del Banco Santander. No me termina de convencer.

También es interesante este artículo de Enrique Dans, en el que habla sobre los nuevos bancos, que llaman "fintech". También es interesante, el enlace que pone a la directiva europea PSD2, una ley aprobara por el Parlamento Europeo sobre los bancos, que hace que las fintech puedan tener cierta ventaja. También es curioso saber que Revolut tiene planeado sacar una tarjeta de débito que te entregará en criptomonedas el 1% de lo que gastes con esta.

3.2 Tarjetas

Actualmente, tengo asociadas a la Cuenta Zero, del Banco Santander, una tarjeta Zero de débito y una tarjeta E-cash, que es una tarjeta monedero, simplemente.

Tengo la aplicación Wallet (del Banco Santander), para poder simular la tarjeta Zero y hacer pagos con el móvil; emplea tecnología *near-field communications* (NFC). También, podría optar por la aplicación Samsung Pay, pero estas dos aplicaciones son mutuamente excluyentes; quizás pruebe la de Samsung algún día. El Banco Santander no es compatible con Android Pay; sí lo es el OpenBank, que es del Banco Santander.

La tarjeta de débito MasterCard que dan con la Cuenta Zero del Banco Santander tiene seguro, cosa que me parece importante.

3.3 Cuenta Zero

Actualmente, tengo la Cuenta Zero, que me permite tener una tarjeta de débito y también puede seguir teniendo una tarjeta monedero. Es una cuenta "100% digital no remunerada", según dicen. A partir de enero de 2018, el Banco Santander cambió las condiciones de sus cuentas. La cuenta que solía tener todo el mundo pasó a tener una comisión de mantenimiento de 3 €/mes. Esto lo hicieron para incentivar a la gente a pasarse a la Cuenta Zero, que te obliga a operar por internet

para casi todo. Esto no quita que pueda concertar una cita en una sucursal para pedir una hipoteca o un préstamo, por ejemplo, al igual que puede hacerlo con un banco con el que no tenga su nómina domiciliada.

A mí, personalmente, me da igual, pues, en todos los años que llevo con la cuenta, he intentado operar siempre por internet. Está claro que, como se dice últimamente, los bancos quieren deshacerse de sus sucursales, pues les están haciendo perder bastante dinero, cosa que no me parece mal. En su web explican las condiciones.

4 Tecnologías de criptoactivos

Actualmente, se está modernizando bastante el mundo de las finanzas. Esto se debe, principalmente, a las **redes P2P de criptoactivos** (también conocido como **plataformas de criptoactivos**), como las basadas en la tecnología blockchain (por ejemplo, Bitcoin es un activo moneda en una red de este tipo).

Aunque seguramente haya oído hablar de Bitcoin, las redes P2P de criptoactivos son algo mucho más general. Bitcoin es en realidad una aplicación de blockchain. Le permite gestionar un activo: una moneda. Existen otras con las que puede gestionar activos de otro tipo: tierras en propiedad, derechos intelectuales de una obra como un libro, objetos virtuales de un videojuego etc. En el mundo de estas tecnologías, suelen llamar **token** a los criptoactivos.

Aunque blockchain es la tecnología que ha producido esta modernización, se está desarrollando también otra tecnología, que llaman *hashgraph*.

4.1 Blockchain

Como hemos dicho, **blockchain** es la tecnología de criptoactivos que revolucionó todo el mundo de las finanzas, y seguramente de otros ámbitos, como la administración pública. Lo que hizo fue incluir la criptografía en las finanzas. Quizás tiene la imagen de un criptógrafo —es decir, un experto en criptografía— como alguien que investiga las tecnologías que permiten transmitir mensajes de forma privada[1], es decir, sin que nadie pueda ver su contenido (*eavesdropping*) ni alterarlo (*tampering*). Para estos fines, los especialistas en criptografía suelen tener conocimientos de matemáticas (principalmente, probabilidad) e informática.[2] Esa imagen se corresponde con la realidad, pero también es cierto que desde

[1] Se suele usar más el adjetivo *secreta* aquí (*secret* en inglés), pero yo prefiero *privada*.

[2] En los comienzos, es decir, hasta la segunda guerra mundial, pensaban que serían los lingüistas quienes debían dedicarse a esto, pero Alan Turing y otros matemáticos demostraron que la criptografía es tarea de matemáticos.

hace mucho han intentado que la criptografía pueda usarse para otros propósitos, como, por ejemplo, para crear una moneda[3] con la que las transacciones puedan hacerse sin la necesidad de que las autorice una autoridad central —en definitiva, una tercera persona—; esta moneda, si se llegase a crear, sería una **criptomoneda**. Dicho de otra forma, una criptomoneda es una moneda (como infraestructura) que se creó teniendo en cuenta la teoría de juegos[4] para que la gente, sin que tenga que intermediar una tercera parte, no tenga incentivos para no cumplir con las transacciones. Gracias a esto, nos podríamos ahorrar muchos intermediarios que necesitamos en nuestro sistema monetario actual.

Así estaban las cosas hasta 2008, en intentos sin éxito de crear una criptomoneda. El gran problema al que se enfrentaron quienes trataron de abordar este reto fue el conocido como "problema de los generales bizantinos", que consistía en cómo alcanzar un consenso entre ciertos agentes sin que tenga que intermediar una autoridad central. Era un problema de matemáticas[5]. Se habían propuesto ciertas soluciones, pero creo que ninguna era práctica. Entonces, una persona (o quizás eran varias) con el apodo (*nickname*) Satoshi Nakamoto (y que no se sabe aún de quién o quiénes se trata) publicó un artículo académico (*paper*) en una lista de criptografía donde explicaba una forma de resolver el problema y la forma de crear una criptomoneda, que se llamaría Bitcoin. El 3 de enero de 2009 se implementó, por un grupo de voluntarios, esa moneda en internet (aunque realmente es una tecnología que podría usarse en otras redes); es un proyecto open source.

En ese artículo académico, se explicaban todos los detalles. Por ejemplo, la forma de resolver el problema de los generales bizantinos sería con una cadena de bloques (*blockchain*) de hashcashes, es decir, una tecnología que se ideó *ad hoc* para poder crear la criptomoneda Bitcoin. No es relevante que conozca los detalles técnicos,[6] lo que sí es interesante es que a esta forma de resolver el problema, dicho de otro modo, a esta tecnología, se la conoce como "cadena de bloques" o quizás más por su forma en inglés: blockchain.

[3] Cuando digo *moneda*, me estoy refiriendo en realidad tanto al token que se asocia con un valor económico como a un medio de pago, es decir, a una infraestructura que facilita las transacciones en las que media el intercambio de dicho token. La moneda puede ser, como token, puramente virtual, es decir, que no tenga la forma de disco de metal con una cara troquelada, sino que es un objeto único que en realidad son datos en uno o varios computadores. En el ámbito de las criptomonedas, hay quien llama a los tokens criptoactivos (*crypto assets*), por lo tanto, una criptomoneda como moneda podría decirse que es un criptoactivo monetario.

[4] La teoría de juegos es una rama de la economía, o quizás, más ampliamente de la sociología, que estudia el comportamiento de las personas en ciertos ámbitos, como, por ejemplo, el mercado de bienes y servicios. La teoría de juegos la creó el matemático John Nash. TKTKTKTK.

[5] creo que de la teoría de grafos. Algunos matemáticos habían conseguido algunos hitos en la investigación de este problema, como, por ejemplo, Leslie Lamport, el creador de LaTeX y que recibió la medalla Turing por sus contribuciones a la teoría de la computación

[6] Puede consultar la explicación de 3Blue1Brown. Es algo técnica pero accesible para casi cualquiera.

En cuanto a la terminología, se suele hablar de "blockchain" a secas cuando nos referimos a la tecnología en sí. Sin embargo, al hablar de una de sus implementaciones (por ejemplo, el de Bitcoin, Ethereum etc.), especificaremos a qué tecnología de criptoactivos en concreto: blockchain de Bitcoin, Ethereum, etc. Creo que hay quien se refiere como "Blockchain" (con *b* mayúscula) al de Bitcoin. Creo que es mejor hacerlo de otro modo, pues podría existir confusión en el lenguaje hablado (no escrito).

Desde entonces, han surgido muchas otras monedas y sistemas de pago que se basan en la tecnología blockchain. También han surgido otras que no usan blockchain y resuelven el problema de otra forma. El tiempo dirá cuál es la que triunfa —quizás ni existe aún la que termine usándose mayoritariamente—, o quizás se usen varias o incluso varíe con el tiempo, como sucede con los cifradores (también conocido como esquemas de cifrado).

Además de una moneda —que también es un sistema de pagos, tal y como dije—, se puede pensar de forma más amplia, pues la economía como ciencia no estudia únicamente las transacciones en las que media el dinero; aunque sí que es una institución/infraestructura... muy importante. Han surgido otros blockchains, como Ethereum, que registran en tokens (también conocido como criptoactivos o, en inglés, *crypto-assets*) todo tipo de cosas: dinero, terrenos, objetos virtuales, etc. Un token se podría decir que es un objeto de software que almacena valor haciendo uso de la criptografía y evita el problema del gasto doble (*double-spending problem*), ese valor puede ser, como he dicho, en forma de dinero, de tierras etc. También permiten hacer contratos que se ejecuten de forma autónoma, pues están registrados en un programa informático: son los **contratos inteligentes** (*smart contracts*).

Uno de los mejores artículos que he encontrado sobre Bitcoin y Blockchain es este. También me gustó este artículo de Chris Dixon sobre descentralización.

4.1.1 Problemas de los blockchains

Existen ciertos problemas en los blockchains que hacen que sea un incordio y se malgasten recursos a la hora de hacerlo funcionar. Aun así, internet también tuvo muchos problemas en sus comienzos, así que no hay que suponer que estos sean irresolubles.

4.1.1.1 Poder de cómputo, energía y tiempo

Una de las tecnologías que es parte fundamental de los primeros blockchains (como en las primeras versiones de Bitcoin y Ethereum) es el proof of work, que se usa para la validación de las transacciones. El problema de emplear proof of work es que se emplea mucho poder de cómputo en la red, y, por tanto, mucha energía, para validar las transacciones. También hace que se tarde mucho tiempo en validar las transacciones.

Por ejemplo, no es práctico, en muchas situaciones, que una transacción tarde en ejecutarse 10 minutos, aunque también es cierto que las transacciones entre bancos (con el sistema que se ha empleado tradicionalmente, conocido como SWIFT[7]) pueden tardar hasta 3 o 4 días.

Posteriormente han salido otras técnicas que podrían sustituir o complementar al proof of work: por ejemplo, el proof of stake. En la versión de Ethereum que saldrá en verano de 2018, tienen previsto usar una mezcla de proof of work y proof of stake. Además, están surgiendo otras tecnologías para complementar a los blockchains y hacer que algunas de las transacciones se realicen de modo más rápido fuera del blockchain. Se las conoce como *off-chain transactions*. La tecnología más conocida de *off-chain transaction* es la Lightning Network, y parece ser que está funcionando muy bien.

4.1.1.2 Anonimato de las transacciones

Otro de los considerados problemas de Bitcoin es que las transacciones no son tan anónimas como desearían algunos. Por ejemplo, muchos bancos de inversión desean que sus transacciones no pueda verlas la competencia, pues perderían una ventaja considerable. Para solucionar esto surgieron algunas técnicas que implementaron algunas criptomonedas como Z-cash; creo que Ethereum también lo va a implementar. En Stellar —que no se basa en blockchain— también son privadas las transacciones. Me guataría recalcar que el anonimato no es para evitar ser espiados por agencias gubernamentales ni para evadir impuestos ni operar en mercados ilegales, sino por razones puramente financieras. Además, el dinero en efectivo (*cash*) es lo que siempre se ha usado para ese tipo de cosas y nadie pide que lo prohíban; aunque también es cierto que con cash no se pueden hacer muchas transacciones rápidamente.

4.1.2 Bitcoin

Bitcoin fue la primera criptomoneda que surgió, pues, en el paper que publicó su creador y donde la presentó, solucionó el principal problema que existía en la investigación para la creación de una criptomoneda, hasta entonces irresoluble. La solución de este problema —conocido como el problema de los generales bizantinos— es el Blockchain, es decir, la tecnología subyacente de Bitcoin. Se puede decir que Bitcoin en realidad no es más que una aplicación de Blockchain. En concreto, el Blockchain, o cualquier blockchain, no es más que una base de datos[8] que se encuentra replicada en muchos nodos (computadores) y que, mediante la criptografía, se registra todo tipo de cosas y no se puede alterar

[7] Esas siglas vienen de Society for Worldwide Interbank Financial Telecommunication.

[8] Muchas veces dicen que es un *ledger*, que creo que es un libro de cuentas. En realidad, blockchain hace alusión a una base de datos.

a menos que cuentes con más del 50% de poder computacional de todos los computadores que forman esa red. Según dicen, su creador hizo un uso muy inteligente de la teoría de juegos para que se pudiera crear la criptomoneda.

Si desea saber algo sobre los aspectos técnicos del funcionamiento de Bitcoin, puede ver este vídeo.

Ya hemos comentado los Problemas de los blockchains. En Bitcoin, se están probando distintas formas de solucionarlo, algunas se han implementado mediante forks de Bitcoin. Por ejemplo, tenemos Bitcoin Cash. Vea también SegWit. También hay quien explica que no es tanto el malgasto de recursos si se compara con el sector financiero al que el Bitcoin sustituiría (dejaría obsoleto), sino que seguramente saldríamos ganando. Además, en 2018 se está actualizando el Blockchain (de Bitcoin) para que haga uso de la tecnología lightning network. Además, los equipos que se encargan de hacer la operación de proof of work (lo que también se conoce como "el minado"), cada vez son más eficientes; si se sigue cumpliendo la ley de Moore, el problema en realidad no sería tan grave.

Otro de los problemas principales que se ha visto que tiene Bitcoin no es tanto técnico como económico: la gente lo usa no como moneda de cambio sino como reserva de valor (*store of value*), como se hace con el oro. Es evidente: si esperas que suba mucho el valor del Bitcoin en relación a otra moneda que uses normalmente, como puede ser el dólar americano (USD), es normal que tus pagos los hagas en USD y no toques los Bitcoins que tienes. Esto, que sucede con otras criptomonedas, en el caso del Bitcoin la hace más propicia a terminar siendo reserva de valor únicamente, porque el diseño de Bitcoin consiste en que habrá una cantidad finita de Bitcoins en el mundo y no se crearán más. Es decir, no tiene un organismo estatal que controle la acuñación (metafórica, claro) de moneda. Hay quien cree que la situación actual lo más probable es que se revierta. Para ello, alude a la ley de Gresham y la de Thier en la economía.

En la jerga de las criptomonedas, suelen llaman **altcoins** a las criptomonedas que no son Bitcoin. Por ejemplo, al analizar la capitalización bursátil del mercado de las altcoins.

4.1.3 Ethereum

Uno de los blockchains más interesantes actualmente es Ethereum. Es un fork de Blockchain que usa un lenguaje Turing-completo mediante el que se podrían crear aplicaciones de software de todo tipo. El Blockchain de Bitcoin, sin embargo, es algo más simple; habría que añadirle capas por encima para conseguir hacer lo que hace Ethereum. También, debido a esto, es más difícil hacer aplicaciones para el Blockchain de Bitcoin. Según Jio Ito (director del MediaLab del MIT), esto es lo que hará que el Blockchain de Bitcoin sea el que termine triunfando, al igual que el protocolo Ethernet y otros que constituyen el internet actual vencieron a

la tecnología que pretendía la industria de las telecomunicaciones, a mediados de los 90, que sustituyera a la incipiente internet. Para él, la simpleza y su diseño en capas (*unbundling*) son una ventaja.

Quienes critican a Ethereum, ponen como ejemplo los escándalos de seguridad que se han dado, por ejemplo, el escándalo del DAO, tras el que terminaron haciendo un hard fork de toda la plataforma.

Una de las cosas que permite Ethereum (que también se podrán hacer con otros blockchains) son los contratos inteligentes (*smart contracts*), que son contratos que se ejecutan de forma autónoma sin que deba intermediar una tercera parte. Piense, p.ej., en una máquina expendedora de bebidas: usted opera con ella mediante un contrato inteligente muy simple cuando compra una bebida.

Al ser Turing-completo, Ethereum es en realidad una máquina virtual que funciona en un cluster de computadores: todos los computadores que están minando. Esta máquina virtual puede ejecutar cualquier tipo de aplicaciones: contratos inteligentes, videojuegos, etc. El problema actualmente es que requiere mucho trabajo computacional hacer cualquier cosa por simple que sea; se espera que la implementación de varias técnicas que modifiquen su funcionamiento en versiones siguientes, sumadas a la esperanza de que se siga cumpliendo la ley de Moore, hagan que sea factible en un futuro operar en Ethereum con comodidad, pero eso es algo que está por ver.

Entre las técnicas para solucionar los problemas de las blockchains, en Ethereum se puede especificar la prioridad que desea para cada transacción: si desea que sea muy rápida, deberá pagar mayor tasa. Creo que a esto lo llaman *gas*.

La moneda de Ethereum se llama Ether (o por su símbolo ETH); técnicamente, dicen que es "el token principal de moneda", lo cual no quiere decir que sea el único token de moneda; cada aplicación podría tener uno propio. En el mundo de Ethereum tienen una jerga un poco especial. Por ejemplo, llaman *token* a todo lo que pueda tener valor que quedar registrado en Ethereum; como dije, se podría llamar también criptoactivo (*crypto-asset*). Por ejemplo, Ether (ETH) es un token. También hay tokens, por ejemplo, que representan las tierras que tienes en propiedad, objetos virtuales que posees en un videojuego etc.

Parte importante de Ethereum, aunque no exclusiva de esta plataforma, son las initial coin offerings (ICO), que es una forma de comprar algunos de los tokens que emite alguna empresa que cree productos o servicios que operen en Ethereum. Sería el eqiuvalente a una oferta inicial de acciones (*initial public offering* o, por sus siglas, IPO), es decir, la salida a bolsa. TKTKTKTKTK.

Creo que, según Vitalik Buterin, el creador principal de Ethereum, la clave está en la descentralización. Por eso cree él que Ethereum es mejor que el blockchain de Bitcoin. Encontré un vídeo donde explica sus ideas sobre la descentralización

Ahora, me gustaría hacer unas pruebas del table mode de Vim:

Entonces...

name	ddress |	phone
John Adams	1600 Pennsylvania Avenue	0123456789
Sherlock Holmes	221B Baker Street	0987654321

Me gustaría hacer una prueba para ver qué tal funciona esto del tema de introducir notación matemática $v_g = i^2 + x^3$. También, Tal y como explican en la tabla tabla-prueba, puede ver que.

$$v_g = \int_0^t \tau^2 \, d\tau.$$

Entonces vemos que... Me gustaría introducir algo de código:

```
polkit.addRule(function(action, subject) {
    if ((action.id == "org.freedesktop.login1.reboot" ||
        action.id == "org.freedesktop.login1.reboot-multiple-
            ↪ sessions" ||
        action.id == "org.freedesktop.login1.power-off" ||
        action.id == "org.freedesktop.login1.power-off-
            ↪ multiple-sessions" ||
        action.id == "org.freedesktop.login1.suspend" ||
        action.id == "org.freedesktop.login1.suspend-multiple-
            ↪ sessions" ||
        action.id == "org.freedesktop.login1.hibernate" ||
        action.id == "org.freedesktop.login1.hibernate-
            ↪ multiple-sessions") && subject.isInGroup("power
            ↪ "))
    {
        return polkit.Result.YES;
    }
});
```

Esto es código JavaScript, como puede ver. También quiero ver cómo queda el código alineado, es decir, `action.id == "org..."` entonces sería `action.id ↪ == "org..."` pero también...

Esto es solo una prueba que estoy haciendo para ver hasta qué extremo llega esto que hemos llamado.

Primera	Segunda Col.	Tercera Col.
la primera	esta segunda	Y terc.
una prueba	esta prueba	y prueba

Esto es solo una prueba.

Esto es una prueba.

4.2 Hashgraph

El hashgraph es la otra técnica que se está empleando para implementar criptomonedas.

Encontré un artículo que explica las diferencias entre hashgraph y blockchain

4.2.1 Stellar

Stellar es una plataforma parecida a un blockchain pero que sigue otra estructura: en lugar de la estructura blockchain (cadena de bloques), usa una estructura de hashgraph; el hashgraph sigue una estructura de árbol[9]. Esta estructura la hace diferente a las blockchains por ejemplo en que todas las monedas están ya preminadas, es decir, que no se van a minar, y que, por tanto, las transacciones se hacen mucho más rápido; actualmente, en menos de 5 segundos.

La moneda oficial de la plataforma Stellar son los Lumens (XLM o, antiguamente, STR). Creo que también hay quien los llama "Stellar Lumens", pero da igual. Existe otra moneda, que es en realidad un submúltiplo de los Lumens: los stroops. La equivalencia es 100 stroops = 0.00001 XLM. Digo 100 stroops porque ese es el pequeño impuesto que se debe pagar a la red por cada transacción, para evitar que haya gente que se dedique a hacer spam dentro de esta, pero que no supone prácticamente un impuesto ya que su valor es ínfimo.

Según tengo entendido, se perdería algo de descentralización con respecto a otras plataformas de blockchain como Ethereum, pero se seguiría considerando descentralizada.

Hay gente de bastante prestigio en el mundo de las fintech, y de las nuevas tecnologías en general, en este proyecto. Por ejemplo, su creador principal es Jed

[9] Al hablar aquí de *árbol*, me refiero a la estructura matemática conocida como *árbol*, que está dentro del campo conocido como la teoría de grafos. Si no me equivoco, esta disciplina está dentro del álgebra. Como aplicaciones, por ejemplo, se tienen el modelo de los circuitos eléctricos sencillos (*lumped-matter discipline*), es decir, un circuito se modela como un grafo. También se aplica la teoría de grafos a muchos de los componentes de los computadores, como, por ejemplo, los sistemas de ficheros, la estructura de software etc.

McCaleb, que fue el creador de Ripple, de MtGox (la vendió antes del escándalo) y eDonkey. En realidad, es un desarrollo open source que es un fork de Ripple, pero, según dicen, lo han mejorado bastante. Además, Ripple es propiedad de una empresa, mientras que Stellar es open source. En el consejo de asesores se encuentran, entre otros, Joi Ito (MIT MediaLab, aunque es más partidario de Bitcoin), Matt Mullenweg (WordPress), Patrick Collison (Stripe) y Sam Altman (YCombinator). Stripe dejó de ser compatible con Bitcoin para pasarse a Stellar. Moxie Marlinspike, creador de la aplicación de mensajería instantánea encriptada Signal y del encriptado de Whatsapp, Skype, etc., tiene previsto sacar una criptomoneda, llamada MobileCoin, en la plataforma Stellar. Al igual que hizo con el cifrado de las aplicaciones de mensajería instantánea, pretende que esa nueva criptomoneda sea muy fácil de usar sin perder la seguridad que debe tener.[10]

Las aplicaciones en Stellar estarían más restringidas al mundo de las finanzas si se las compara con las de Ethereum. No usaría un lenguaje Turing-completo. Lo bueno, según dicen sus creadores, es que serían más seguras y además más sencillas de crear. Olvídate de jugar a videojuegos que corran sobre Stellar: el videojuego correría en tu máquina y, en todo caso, las compras de objetos sí se harían en la red Stellar.

Esta puede que sea la mejor explicación de Stellar que he visto. También puede ver este vídeo, que se centra más en la parte financiera. También encontré una explicación de por qué es posible que se revalorice Stellar en 2018. Han publicado su roadmap de Stellar para 2018.

4.3 Gestión

4.3.1 Wallet

Un **wallet** (o cartera) es una aplicación que sirve de cartera digital para una o varias criptomonedas. Es decir, el wallet contiene un fichero que le permite certificar que usted posee una cantidad determinada de cierta moneda. Este fichero solo podrá usarlo realmente quien tenga la clave asociada. Ahora no estoy seguro de si es así. Creo que en realidad, mi dinero está en todos los nodos de la red Bitcoin (o la que sea); lo que almacena el wallet es mi clave privada, que permite que yo pueda hacer transferencias con mis tokens Bitoins (o de lo que sea).

[10] En concreto, consiguió que las aplicaciones de mensajería instantánea (IM) usasen el protocolo Signal, que es algo así como el viejo PGP pero mucho más cómodo de usar, pues por cada conexión se usa una clave distinta: no tiene que estar almacenando las claves públicas de todas las personas con las que se comunica. Es también de encriptado de extremo a extremo. Su aplicación de IM, llamada Signal, usa ese protocolo y es open source. Después, las más conocidas la copiaron y también usan ese protocolo, como, por ejemplo, WhatsApp, Facebook Messenger, Google Allo y Skype.

Existen varios tipos de wallets: online, offline, hardware y cold.

4.3.1.1 Wallet online

En los online wallets, el wallet, es decir, el fichero, se almacena en la nube de este servicio de internet y usted accede al mismo mediante su clave. El online wallet más conocido es Coinbase, que es, sobretodo, un exchange. Los online wallets han dado problemas, pues algunos servicios de este tipo han sido hackeados y les han robado los ficheros de los wallets. Según un post en el subreddit de Bitcoin, lo mejor es no fiarse de los online wallets. Otro de los inconvenientes de los online wallets es que, en ciertas situaciones, pueden congelar las operaciones. Por ejemplo, si empieza a caer mucho el precio de una criptomoneda y los inversores entran en pánico, puede que el wallet online no le permita sacar su dinero en ese momento. , en mi humilde opinión, no merece la pena hacer *daytrading* con criptomonedas. Creo que lo que se debe hacer es invertir a largo plazo en una que crea que tiene futuro, sin obsesionarse ni estar mirando constantemente su valor; invertir a muy largo plazo, con intención de, si es posible, no llegar a sacarlas nunca sino esperar a que termine siendo un medio de pago a nivel mundial muy reconocido.