TRABAJO FIN DE GRADO

ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

# TECNOLOGÍA BLOCKCHAIN, SMART CONTRACTS y CASO SWAP.

---

DESCRIPCIÓN, EVOLUCIÓN, APLICACIONES y TENDENCIAS


**Autor**

Ferran Vilar Pagès

**Tutor**

Dr. Eudald Puig

Departamento de Organización i Administración de Empresas


UNIVERSITAT DE BARCELONA

Facultat d'Economia i Empresa
Universitat de Barcelona

2019 - 2020

RESUMEN EJECUTIVO

La tecnología blockchain, descentralizada, inmutable, segura y anónima, ha generado gran expectación para con sus posibilidades de aplicación en distintos sectores como el financiero, el turismo, el Internet de las cosas (IoT), la sociedad y los sectores públicos. Si bien existen estudios y trabajos que respaldan una reestructuración de la economía tal y como la conocemos hoy en día, es de opinión dispar las posibilidades y el rango de afectación de la tecnología en la realidad. Para intentar reducir esta discrepancia de posiciones con respecto a su futuro, se analizan sus bases desde su ejecución por primera vez en 2009, junto al funcionamiento que sigue. Será objeto de estudio su evolución en el tiempo, la afectación de esta a un servicio financiero, la aplicación en distintos sectores y la exposición de sus limitaciones en la actualidad. Así mismo, este trabajo menciona alguna de las tendencias futuras de la tecnología blockchain.

PALABLRAS CLAVE: Blockchain, Minero, Hash, Token, Bitcoin, Smart Contract, Duración, Ethereum, Desarrollador y PoW.

EXECUTIVE SUMMARY.

*BLOCKCHAIN TECHNOLOGY, SMART CONTRACTS and SWAP CASE.*
*Principals, Evolution, Applications and Future Trends*

The blockchain technology, decentralized, immutable, anonymous and secure, has generated great expectations for its potential application in various sectors such as finance, services, the Internet of Things (IoT), society and public sectors. Although there are studies and works that support a restructuring of the economy as we know it today, the possibilities and the range of impact of technology in reality is of different opinion. To try to reduce this discrepancy of positions regarding its future, we analyze its bases since its execution for the first time in 2009, its principals such as architecture of the chain, the different participants it can suit and the benefits they bring to the network as a whole, along with the functionality it follows. Its evolution over time, the way in which it has affected a financial service to exemplify the power to make inference in reality the new abilities have, the implications it has within real projects such as, supply chain management. Also, some other sectors will be mentioned as eligible to adopt a blockchain system in order to gain insights against the competence and the exposure of the current limitations will be studied. Furthermore, this work points out some future trends of the blockchain technology.

KEY WORDS: Blockchain, Miner, Hash, Token, Bitcoin, Smart Contract, Duration, Ethereum, Developer and PoW.

# INDICE

**I. INTRODUCCIÓN ..... 5**

**II. ¿POR QUÉ TODO ESTE REVUELO? ..... 7**

**III. TECNOLOGÍA BLOCKCHAIN: DESCRIPCIÓN ..... 9**

1. BLOCKCHAIN: ARQUITECTURA ..... 9
*1.1 Bloque ..... 10*
2. TRANSACCIONES Y FIRMA DIGITAL. ..... 11
3. CARACTERÍSTICAS DE LA BLOCKCHAIN. ..... 12
4. FUNCIONAMIENTO DEL SISTEMA BLOCKCHAIN. ..... 14
5. EL ALGORITMO DE CONSENSO ..... 15

**IV. TECNOLOGÍA BLOCKCHAIN: EVOLUCIÓN. ..... 18**

1. DE TRANSACCIONES A SMART CONTRACTS. ..... 18
2. APLICACIÓN FINANCIERA: SWAP DE TIPO DE INTERÉS ..... 19
3. SMART CONTRACTS. DESCRIPCIÓN ..... 21
4. COMO FUNCIONAN LOS SMART CONTRACTS ..... 23
5. ORACLE: LA PLATAFORMA *CLOUD* DISTRIBUIDA ..... 24
6. ETHEREUM. ..... 27
*6.1 Ether ..... 28*
*6.2 Cuentas Ethereum ..... 28*
*6.3 El precio del Gas o ETH ..... 29*
7. LAS DIFERENCIAS ENTRE BITCOIN Y ETHEREUM. ..... 30

**V. TECNOLOGÍA BLOCKCHAIN: APLICACIONES ..... 32**

1. EL IMPACTO DE LOS SMART CONTRACTS. ..... 32

**VI. LIMITACIONES DE LA TECNOLOGÍA BLOCKCHAIN ..... 37**

1. COMPARACIÓN Y EL TRILEMA DE SEGURIDAD-DESCENTRALIZACIÓN-ESCALABILIDAD ..... 41

**VII. ¿CUÁL ES EL SIGUIENTE PASO? ..... 44**

**VIII. CONCLUSIONES ..... 45**

**IX. BIBLIOGRAFÍA ..... 47**

**X. WEBGRAFÍA ..... 48**

**XI. ANEXO ..... 49**

# I. INTRODUCCIÓN

"*Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for the model transactions, it still suffers from inherent weakness of trust-based model. […] What is needed is an electronic payment based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party*."

*(Nakamoto, 2008)*

El misterioso *white paper* bajo la autoría de Satoshi Nakamoto describía y sentaba las bases de un modelo de criptomoneda totalmente distribuido, basado en una cadena de bloques capaces de almacenar cualquier tipo de datos juntados por una cadena criptográfica. No fue hasta 2010 que este sistema se hizo realidad fomentando la carrera para escalar la cima del *Bitcoin*, vigente a día de hoy. Doce años después de su puesta en escena, las innovaciones que este presentaba lideran el siguiente escenario de las conexiones digitales, abriendo puertas a un espacio compartido, descentralizado, confiable y de conformidad distribuida.

La funcionalidad de la cadena de bloques criptográfica, a partir de ahora *blockchain*, se explica con lo que a día de hoy sigue siendo se principal activo, el Bitcoin[1]. Los conceptos usados para la explicación y la puesta en marcha de la primera criptomoneda no eran innovadores como tal, si bien la idea y la forma de almacenar datos que plantea la tecnología blockchain tiene antecedentes muy anteriores, en la década de los 70: las bases de SQL; vigente para instituciones centralizadas. Lo que sí fue rompedor eran las posibilidades que su interconexión producía que habilitaron un espacio para realizar transacciones entre individuos de forma anónima y confiable. Introdujo lo que se conoce como *trusted network*. Por primera vez en la historia se hacía realidad un sistema que permitía hacer transacciones sin necesidad de la participación de terceros agentes generadores de confianza permitiendo así una relación entre individuos. Hacía con ello posible lo imposible. (Navarro, 2017)

El concepto blockchain no es demasiado intuitivo, por lo que hace necesario un conocimiento extenso de las partes que engloba y como estas actúan de forma sinérgica. Esta dificultad de comprensión aflora disparidad de opiniones por lo que al futuro concierne, hay quienes creen que será un punto de inflexión, no solo en las transacciones de dinero, sino como un modelo alternativo que suprimirá el poder monetario de los gobiernos centrales, conduciendo a una nueva era de libertad económica e independencia, y otros, son cautos, y no le ven más

[1] Bitcoin no es identidad de Blockchain. Son dos conceptos muy distintos y sería un error tratarlos por igual. La tecnología Blockchain es condición sine qua non de Bitcoin.

posibilidades lejos de las transacciones de valor. Solo el tiempo y la innovación tecnológica saben el rumbo que tomará. (Nofer, 2017)

Una cosa es clara, si las expectativas que se generan con esta nueva tecnología devienen reales, estaremos ante una revolución tecnológica. Se espera esta lleve consigo un cambio rápido de las tendencias y una repercusión al medio-largo plazo a gran escala. Ciertamente podría ser esta la tecnología del futuro, pero cabe la posibilidad que todas las expectativas fueran, en su mayoría solo eso en el día de mañana. (Mattila, 2016) (Navarro, 2017)

# II. ¿POR QUÉ TODO ESTE REVUELO?

Hoy en día la transmisión de información de un lado a otro del planeta se puede llevar acabo gracias a la evolución del ordenador y la introducción de internet como puente de contacto. De esta revolución se deriva la problemática de la fiabilidad de la información que se recibe y se comparte. ¿Cómo se verifica que la información recibida es auténtica y actualizada? La cuestión responde a una confianza necesaria entre partes. Aparecen así las organizaciones centralizadas que actúan como terceros agentes entre las partes como mediadoras generando una confianza no necesariamente implícita entre actores. De esta forma soportan el riesgo derivado del acuerdo entre las partes a cambio de una contraprestación económica por el servicio realizado. La actividad de los mediadores era necesaria para habilitar una relación entre individuos. (p. ej. Banco como intermediario en una firma de pagaré entre dos empresas.)

La tecnología blockchain como agente disruptivo ha despertado tanto interés porque tiene la capacidad de facultar una confianza entre partes sin necesidad de terceros involucrados. Propone un sistema de almacenamiento de datos confiable y verificable en todo momento por cualquier usuario de la red. De este modo la participación de un actor ajeno se ve sustituida por la funcionalidad de la misma red.

Para saber que es exactamente lo que la tecnología blockchain permite, uno ha de entender que la sociedad necesita la participación de entidades centralizadas como mediadores en cualquier actividad por la confianza que esta transmite a todo el colectivo. Una confianza necesaria que ha desembocado en ciega. Por ejemplo, se confía en que un repartidor usará tu dirección solo para la entrega de un pedido y que empresa de repartos la usará solo con fines profesionales y en ningún caso de forma fraudulenta. De alguna manera se espera que esa información sea usada solo en el contexto para lo que ha sido facilitada, cuando realmente lo que se permite es la cesión de datos personales de utilidad para las grandes corporaciones centralizadas, pero de incalculable valor para el individuo. La tecnología blockchain cada individuo sería dueño de su información y se daría acceso a ella dentro de un espacio de confianza que previera su mala praxis. (Navarro, 2017)

En su conjunto, blockchain esta cambiando la sociedad desde distintos ángulos. Una de ellas es la construcción de una plataforma totalmente distribuida que genere confianza a los participantes por su condición criptográfica desincentivando así la participación de terceras partes en las relaciones entre individuos y la eliminación de grandes corporaciones centralizadas empoderadas. Con ello blockchain introduce una nueva pregunta en la discusión económica: ¿Cómo crean valor las cadenas blockchain y quien o cómo se genera esta confianza? (Nofer, 2017)

Por otra parte, dentro de la economía industrial en la que se encuentra la sociedad desde su introducción, la tecnología blockchain propone soluciones eficientes a lo que la necesidad de relación entre entidades centralizadas se refiere. Si bien una industria o una empresa puede parecer desde fuera un engranaje que funciona de una manera óptima, ve como la necesidad de acceder a datos o recursos de otras resulta en ineficiencias en forma de tiempo y dinero. Un ejemplo para poner en contexto esto sería el hacer un cambio de domiciliación de la nomina de una entidad financiera a otra. Con el sistema tradicional se tardarían días y sería costoso para el cliente, con una tecnología blockchain se presume esta sería casi inmediata.

Con este efecto doble, blockchain pretende llegar a toda la sociedad, romper con lo establecido dentro de un contexto industrial y que esto se traduzca en un mayor bienestar de toda la población. Una cosa es clara, la tecnología precisa de un proceso de adaptación que, lejos de ser rápido, está siendo sostenido y constante en el tiempo. Existen, por eso, limitaciones tecnológicas y de conocimiento con las que lidiar para poder avanzar hacia un nuevo futuro, y si bien las innovaciones presentadas son esperanzadoras, se ha de probar su impacto real y lo más importante, se ha de producir una aceptación del colectivo social en su totalidad.

# III. TECNOLOGÍA BLOCKCHAIN: DESCRIPCIÓN

Según apunta Roger Wattenhofer, profesor en la *Swiss Federal Intitute of Technology (ETH), "La tecnología Blockchain está formada por dos componentes esenciales, la Criptografía Asimétrica y las Distributed Ledgers"*. Las últimas son la capacidad de interacción de manera distribuida entre participantes, que en su esencia son ordenadores.

Para comprender el poder disruptivo de la tecnología blockchain se procede a la exposición y explicación detallada de cada uno de sus componentes. Es importante destacar que el siguiente análisis se basa en el primer modelo blockchain presentado por Satoshi Nakamoto en 2008. Se conoce como blockchain 1.0.

## 1. Blockchain: Arquitectura

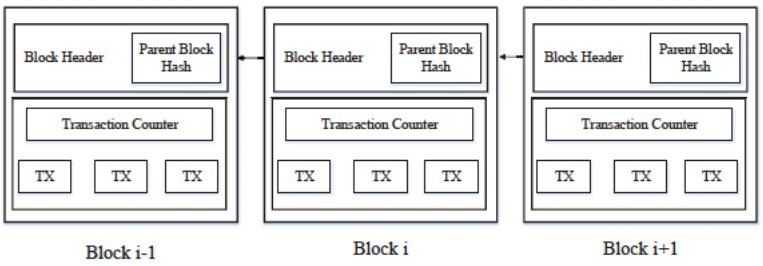



Figura 1: Cadena de bloques criptográficamente unida. Fuente: Zheng, Z. X., 2017

La cadena blockchain es una secuencia de bloques dotados de una serie de datos almacenados en ellos, actuando esta como una base de datos que recuerda a modelos ya existentes. En la figura 1 se presenta la estructura típica de una blockchain. Los bloques están unidos uno a otro de manera secuencial, por lo que un bloque depende de la información que hereda del anterior. Esta anatomía se repite sucesivamente hasta el *Genesis Block* que no le precede ningún otro. La información heredada se encuentra criptográficamente detallada en el *block header*. El valor que resulta del *block header* se denomina *hash,* un valor criptográfico único e irrepetible. Solo se añadirán a la cadena los bloques que se identifiquen como los únicos capaces de relacionar su información con la del antecesor y representar la realidad. (Zheng Z. X., 2017)

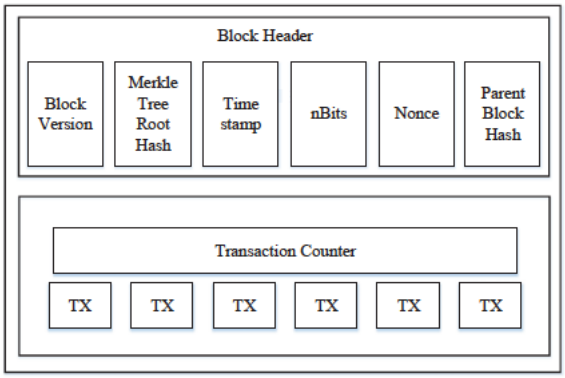



Figura 2: Información contenida en un bloque criptográfico. Fuente: Zheng, Z. X., 2017

### 1.1 *Bloque*

El bloque se constituye en esencia de dos partes: el *block header* y el *block body*. (figura 2)

El *block header* o nombre del bloque registra la siguiente información:

- *Block Version*: Un código alfanumérico que indica las reglas a seguir para la validación del bloque.

- El *Markle Tree Root Hash* que referencie todas las transacciones cabidas en el bloque, un *Time stamp* referencia temporal del hallazgo del hash, *nBits* valor hash de forma compacta y el *Nonce* que incrementa a medida que se sucedan los cálculos del algoritmo hash. (figura 3)

- *Block Parent*: Otro código alfanumérico que permitirá la unión de todos los bloques consecuentes a este. Recogerá de forma compacta los 256 valores del hash del bloque anterior.

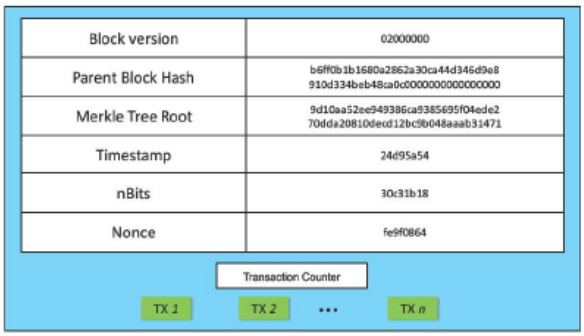



Figura 3: Resultado *hash* ejemplo para un bloque. Fuente: Zheng Z. X., 2018

El *block body* está compuesto por el número de transacciones y el valor de las mismas. El número de transacciones que puede registrar un bloque dependerá de las limitaciones que su red tenga. Para el caso de Bitcoin la limitación se encuentra en el número de transacciones, si bien existen otras, como se verá más adelante donde la limitación reside en la cantidad de criptomonedas a registrar en su totalidad. Para realizar el proceso de validación de cada transacción, blockchain utiliza la criptografía asimétrica basada en una firma digital. Esto se usa en espacios donde no se genera confianza entre participantes. (Zheng Z. X., 2018)

## 2. Transacciones y Firma digital.

Para que se produzcan las transacciones de activos en la red, ésta precisa de dos componentes, los usuarios y la encriptación. Los primeros serán los encargados de realizar la transacción a la que se le asignará un valor hash único e irrepetible gracias al segundo actor, la encriptación. Una vez validada la transacción será añadida al bloque en forma de información criptográfica TX. La participación de los nodos no termina aquí, ya que cuando un bloque es validado y pasa a formar parte de la cadena de bloques, todos reciben una copia actualizada de la misma en su dispositivo para que sea auditable en todo momento.

Cuando se decide ser partícipe de una red blockchain, como usuario se recibe una *private key* y una *public key*. Las llaves privadas se usan para firmar las transacciones y encriptar el valor hash de la misma de forma automática una vez esta es emitida. Las transacciones son globalizadas dentro de la plataforma, por lo que cada usuario puede relacionarse con cualquier integrante de la misma. Cuando quiera efectuarse una transacción deberá constar a que llave pública se quiere enviar. A efectos de la blockchain de Bitcoin, la llave pública es la dirección de cartera de los usuarios.

La transacción entre dos usuarios de la red consta de dos fases: La firma de la transacción y la validación de la misma. (figura 4). Cuando un usuario emisor realiza una transacción, se le deriva un valor hash único e irrepetible. Es con la llave privada que se encripta[2] dicho valor y lo envía dirección a la cartera referenciada. El receptor usa su llave pública para desencriptar el documento obteniendo un valor hash, que a su vez ha de coincidir con el valor que encuentra el validador de la transacción para que esta sea reconocida por la red como real. Si no coincidieran los valores sería debido a que el contenido inicial de la misma ha sido modificado, por lo que no se validaría la operación y quedaría nula de cualquier efecto. En este caso el emisor recuperaría su posición o *state* inicial dado que se le devolvería la cantidad emitida, UTXO.

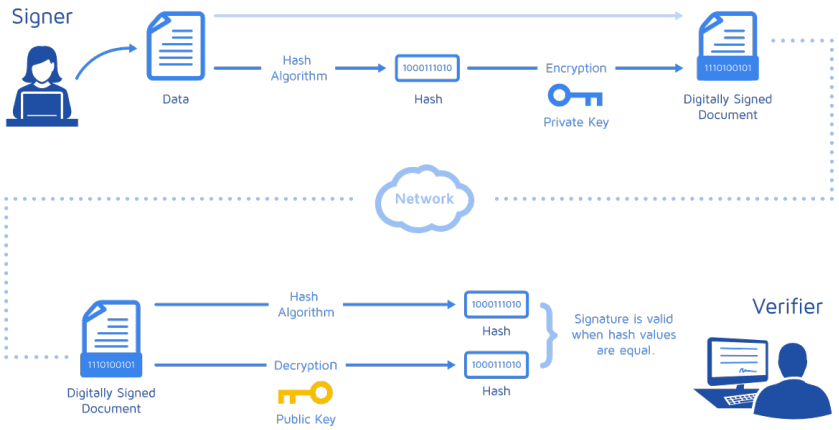



Figura 4: Procesos a los que ese somete una transacción en la red Bitcoin. Transacción completadad

La transacción una vez validada es almacenada en un *Transaction Counter* en el que se depositan todas las validadas. Gracias al sistema *Markle Tree* se relaciona de forma continuada parejas de valores hash de cada transacción validada, culminando en un único valor, el *Root Hash* que contiene información de todas las subyacentes. Se idea un sistema eficiente y trazable para comprobar en todo momento cualquier aspecto de una transacción que se produjo. Dada la relevancia del *Markle Tree*, se recupera en el apartado del algoritmo de consenso. (Nakamoto, 2008) (Xiao, 2020)

## 3. Características de la Blockchain.

- Descentralización: Otorga significado a la creación de la red en si y las hace escalables y con relaciones *peer-to-peer*[3]. Permite la ausencia de confianza entre emisor y receptor, y la hace depositar en la tecnología. Junto a la inmutabilidad de la red de bloques y la réplica masiva automatizada de la cadena una vez

[2] Se ha de entender encriptación como la firma que constata el origen de la transacción
[3] Peer-to-Peer: De un individuo a otro, sin intermediarios.

actualizada a todos los usuarios, blockchain elimina los riesgos de seguridad y manipulación de datos que existen en las organizaciones centralizadas. (Zheng Z. X., 2018)

En un sistema tradicional centralizado todas las operaciones son validadas por una única organización de confianza para todos los usuarios (p. ej. Banco). Si bien cada organización, bancos para seguir con el ejemplo, son eficientes, su necesidad de relación con otras industrias les hace incurrir en un proceso ocioso que genera costes en forma de tiempo y dinero a soportar por el cliente final. Es equiparable, para una mayor comprensión, a un sistema de engranajes donde por mucho que el sistema individual sea óptimo, si la fuerza motriz que conecta una con otra es defectuosa, todo el conjunto lo será.

En cambio, una transacción en una red blockchain recibe la característica *peer-to-peer* porque obvia la necesidad de autentificación por parte de ningún tipo de organización o industria, descentralizando su ratio de acción. Esto se traduce en un ahorro económico y en eficiencias de tiempo para los usuarios.

- Inmutabilidad: Se apuntaba junto a la descentralización de la red. Es estadísticamente muy poco probable cambiar lo que ya ha sido registrado en la cadena. Todo bloque añadido se presume único y representativo de la realidad para todas las transacciones que contiene, lo que resulta en una desincentivación de actividades fraudulentas. (Zheng Z. X., 2018). Nakamoto lo ejemplifica como una distribución de Poisson que pierde consistencia de forma geométrica a medida que aumentan el número de usuarios de la misma.

- Anonimidad: Cada usuario es referido por la llave pública que posee, su dirección de cartera, no por su persona. Es más, si algún usuario quisiera reducir su exposición a la red, podría crear más de una cuenta para usar distintas llaves públicas. blockchain no puede, por eso, garantizar una privacidad total debido a distintas limitaciones que de sus características se derivan. (se explica con detalle en la sección VI).

- Verificable: Toda transacción realizada es validada con un *time stamp* que indica el momento temporal en el que se produjo la validación, quienes eran las partes involucradas y con el sistema *Markle Tree* todas ellas quedan relacionadas entre si. En la blockchain de Bitcoin, por ejemplo, aparece el saldo de cartera de ambas partes antes y después de la transacción y el enlace a las anteriores que verifican

la cuantía presentada. Por lo tanto, es un sistema de búsqueda que resulta en la transparencia total de los datos que se almacenan. (Navarro, 2017)(Anexo 1)

## 4. Funcionamiento del sistema Blockchain.

Los modelos actuales de cadenas blockchain se pueden dividir en dos grandes grupos: Las redes públicas *permissionless* y las privadas o *permissioned*. Cada una de ellas con distintas características de funcionamiento que se detallan en el apartado VI. Para el caso que concierne, el sistema de criptomonedas Bitcoin que propone *Satoshi Nakamoto* es uno público. Como tal, la confianza es depositada en la tecnología detrás de la red blockchain, que ve incrementada su seguridad cuanto mayor sea el número de usuarios participantes de la verificación de las transacciones y los bloques. Son los denominados nodos mineros o *miners.* Para garantizar la seguridad dada la posible participación de cualquier individuo que así lo desee, las redes públicas precisan de un proceso de validación llamado *Proof of Work (PoW),* que sin ir más lejos culmina con un valor hash aceptado por la red. (Nakamoto, 2008). Garantizando así la realidad de las operaciones y evitar manipulaciones para el beneficio de nodos malignos. Se considera a toda la red por igual, y para finalmente añadir un bloque a la cadena una vez encontrado el *Block Hash* del mismo*,* ha de manifestar su aceptación el 51% de la red, siendo este su modelo de consenso.

Algunas veces el proceso de validación de bloques, al ser simultaneo para toda la red, puede darse el caso de que más de un minero encuentre el valor *nonce* apto para el valor hash al mismo tiempo. Como se ilustra en la figura 5, se registran todos los bloques encontrados formando así la denominada *fork*, *branches o* horquillas. El sistema de validación *PoW*, asume como valida la cadena más larga de bloques, dado que es poco probable una asunción de bloques de forma continuada en el tiempo. (Zheng Z. X., 2018)

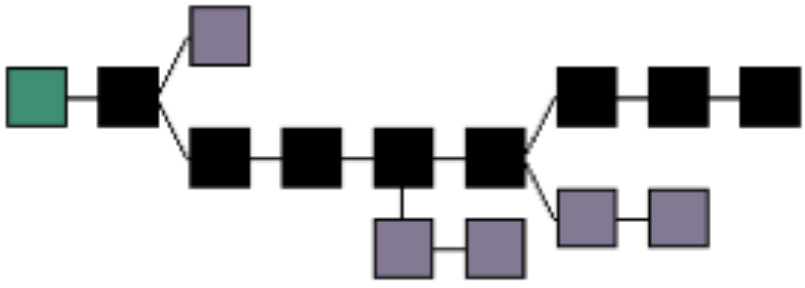


Figura 5: Cadena de Bloques. Fuente: Navarro, 2017

Supongamos dos horquillas generadas simultáneamente y añadidas a la red. Los nodos siguen trabajando y añaden un nuevo bloque a la cadena (negros), haciendo que los

nodos trabajando en la horquilla morada dejen de hacerlo para trabajar sobre la cadena más larga dejando esta huérfana u *orphan block*. La probabilidad de que se siga generando una y otra vez el mismo bloque simultáneamente es poco probable. Los bloques en la cadena de Bitcoin son generados cada 10 minutos. Si un bloque es generado, verificado y añadido a la red en un menor tiempo, el mismo proceso para encontrar el siguiente se actualizará para que sea más laborioso de encontrar para así siempre mantener los 10 minutos y no propiciar un auge de bloques no pertenecientes a la cadena principal. (Navarro, 2017)

Todo el trabajo que realizan los nodos para mantener la veracidad y transparencia de la cadena es consecuencia directa de su trabajo computacional o *CPU work*, y tiene como único objetivo el de mantener la fisionomía del sistema de seguridad y consenso ideado por Nakamoto ante posibles atacantes o potenciales fraudes dentro de la misma.

## 5. El algoritmo de Consenso

Los mineros son los encargados de generar nuevos bloques para la cadena. Cada bloque permite llevar a cabo un registro público de todas las transacciones que se han realizado en un periodo concreto, almacenadas de forma *Markle Tree*, en honor a su creador: Ralph Markle. (Nakamoto, 2008). El proceso para añadir un bloque nuevo, y que este sea de aceptación consensuada es el que sigue.

Los mineros trabajan con la información criptográfica del bloque anterior, el *Parent Hash*, el *nBits* que se indique por el algoritmo, el *Markle Tree Hash Root* que agrupa los valores hash de las transacciones validadas, culminado en el *Root Hash,* como se ilustra en la figura 6, y registrarlo con el fin de reducir el espacio ocupado por cada transacción emplazando así muchas más de las que se podrían si se almacenaran todas y cada una de ellas de forma individual. (Navarro, 2017). El *Nonce* ha de coincidir con ciertos aspectos relacionados con la dificultad de encontrar el valor hash del bloque y una marca *Time stamp* que indica cuando se encontró el valor en cuestión sea este válido o no. Este método de prueba y error que realizan los nodos mineros de una red pública es el llamado *SHA-256* por los 256 caracteres de los que se forma. (Zheng Z. X., 2017)

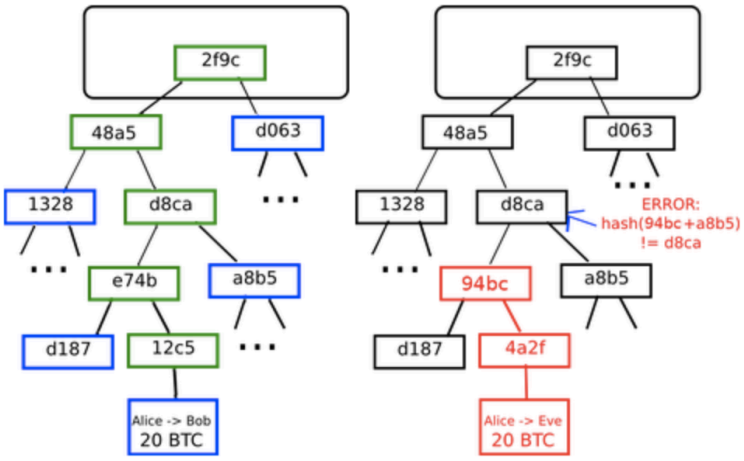



Figura 6: Proceso *Markle Tree Root Hash.* Fuente: Buterin, 2014

Cuando un minero encuentra el hash, los demás han de validar dicho valor. Para llegar a validar un bloque la mayoría de representación de la cadena, el >=51% de los mineros, ha de consensuar que este es la única representación de la realidad. Una vez probado que las transacciones son validas y que el *target value* es el auténtico, se considera que hay consenso y se añade el bloque a la red codificado por el valor hash encontrado. Por último, se distribuye la nueva cadena actualizada a todos los ordenadores participantes de la misma. (Zheng Z. X., 2017)

La estrategia de consenso PoW precisa de complicados cálculos para encontrar valores hash tanto para transacciones como bloques. (Nakamoto, 2008) Para que todo el proceso sea rentable para los mineros, ya que en definitiva el POW se traduce en fuerza *CPU* y gasto de energía por su parte, Nakamoto propone un sistema de incentivos a aquellos que encuentren los valores auténticos. En la red Bitcoin el incentivo es una cierta cantidad de la misma criptomoneda o *token*, directamente ligada a la dificultad y, por lo tanto, requerimiento energético que se deriva de encontrar el *target value* de un bloque. Para el proceso de validación de transferencias se recompensa con un pequeño monto de la misma, también relacionada con la dificultad (Swanson, 2015). Cuánto mayor sea el número de mineros, más probable es que estos sean honestos y menor es la probabilidad de que la red sufra un ataque. (Nakamoto, 2008)

En esencia, la tecnología blockchain 1.0 ofrece un sistema de base de datos distribuida que junto a la criptografía y la informática permite generar confianza entre usuarios a través de la tecnología en la que sienta sus bases. La información, una vez validada e insertada en la cadena es inmutable y compartida en toda la red, consiguiendo así que todos posean la única copia

válida de la cadena. Esto permite que sea transparente, ya que cualquier usuario puede ver y revisar las transacciones registradas en la base de datos, si así lo desea. La base de datos y su autenticidad es sólida gracias a que todos los nodos tienen la única representación real y valida, actualizada gracias a los mineros, permitiendo así que no exista una centralización de la información. En la misma línea los nodos son tratados de la misma manera, no hay jerarquía, lo que resulta en una incorruptibilidad del sistema. (Pilkington, 2016) (Mattila, 2016)

# IV. TECNOLOGÍA BLOCKCHAIN: EVOLUCIÓN.

Lo que en 2008 salió a la luz por parte de la desconocida figura escondida bajo el nombre de Satoshi Nakamoto no fue más que el principio de algo de incalculable valor para la sociedad en su conjunto. Con Bitcoin el concepto de la descentralización se hacia realidad ante los ojos de todo un mundo, en el que solo unos cuántos supieron reconocer el potencial real que este escondía frente al insaciable afán de riqueza y dinero de la mayoría. (Buterin, 2014). Satoshi lanzó así un mensaje implícito más allá de las monedas o de una riqueza palpable, donde se presentan los bloques como forma de tratar y almacenar cualquier tipo de valor y, Vitalik Buterin fue uno de los que lo supo ver.

## 1. De transacciones a Smart Contracts.

Con la revolución tecnológica que supone la Blockhain y sus propuestas, llega la Blockhain 2.0 de la mano de Vitalik Buterin, con la que no solo es posible tener una red pública, descentralizada, segura y confiable por todos sus usuarios, sino que permite la ejecución de código y programas de forma descentralizada y la implementación de los contratos inteligentes o *Smart Contracts*.

Los Smart Contracts son programas automatizados que contienen un conjunto de condiciones que se traducen en ciertos resultados o *outcomes* según la información que se les introduce. (Kehrli, 2016). Esto presenta toda una revolución, dado que las redes blockchain 1.0 no eran programables y se limitaban a una simple interfaz de código. (Nakamoto, 2008) (Anexo 1)

En una transacción entre dos participantes en la red de Bitcoin, primero se ha de comprobar que la parte que quiere enviar dinero, tenga dicha cantidad como mínimo, y si es así, se la ha de restar a uno y sumársela a la parte que la recibe. Solo se hará efectiva la transferencia si se verifica que A puede hacer frente a la transferencia. Con esto el lector entiende que la plataforma Bitcoin, como ejemplo de la red blockchain 1.0, podía ejecutar código, pero este era limitado a la casuística anterior y sin posibilidad de ser cambiado. (Anexo1)(Zheng Z. X., 2017)

Con la blockchain 2.0 el usuario puede ejecutar transacciones de valor de forma, condiciones y características personalizadas, y por tanto adaptadas a las necesidades y preferencias de todas las partes que firman. De este modo, y siendo fiel a la razón de ser de la blockchain, la gran mayoría de operaciones financieras evolucionan a una relación *peer-to-peer.* (Kehrli, 2016)

## 2. Aplicación Financiera: SWAP de Tipo de Interés

Para poder plasmar de forma empírica las ventajas de usar un Smart Contract en lugar de acogerse al método tradicional, se propone un ejemplo de una operación SWAP asociada al riesgo inherente de tener activos y pasivos a tipo de interés distintos a efectos de riesgo y madurez. Se presenta un SWAP de tipo de interés. El ejemplo quiere demostrar que, ante una decisión tradicional, existe una alternativa real de Smart Contract mucho más rápida y menos costosa.

Considere dos empresas: La primera, denominada A, ha ampliado su capital mediante la emisión del equivalente a 100 M € en obligaciones a 4 años, generando estas un pago semestral de un 10% anual fijo sobre el nominal en forma de cupones. Para los activos ha adquirido propiedades que arrenda a menos de un año por lo que piensa percibir anualmente un interés de EURIBOR + 2%.

Como resultado de tener diferencias en los tipos de interés para el activo, variables, y para el pasivo, fijas, la empresa A tiene una brecha de Duración[4] negativa; la duración de su activo es menor que la de su pasivo. Tal que así:

$$Da - kDp < 0$$

Para cubrirse de la exposición al riesgo de tipo de interés la empresa podría hacerlo directamente con su balance o fuera de él. Podría atraer capitales ajenos, pero esta vez indexados al tipo de interés del EURIBOR, lo que llevaría consigo una reducción de la duración y por lo tanto exposición al riesgo, pero aumentaría el nivel de deuda contraída. Supongamos el mercado ofrece deuda indexada EURIBOR + 2,5%. De forma alternativa la empresa A lo que puede hacer es acudir al mercado y vender u ofrecer la posición fija de sus obligaciones.

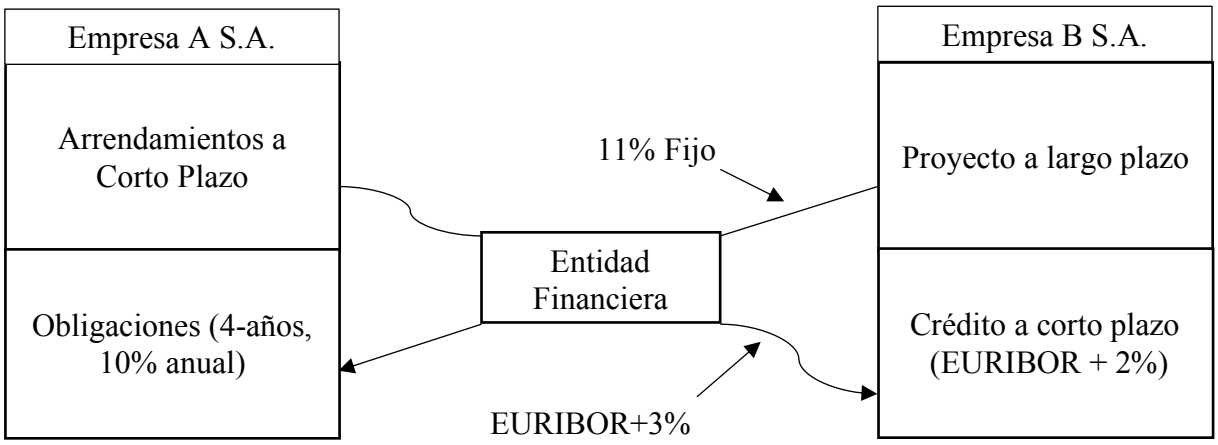
La segunda parte, empresa B, decide acudir al mercado para cubrir su posición corta de pasivo ante una posición larga de activo a interés variable. La empresa B dispone de un capital de 100 M € financiado de forma ajena, a través de entidad bancaria, el cual ha de devolver en un año a tipo de interés EURIBOR + 2% y lo invierte en un proyecto que le proporcionará una rentabilidad anual fija. Quiere cubrirse pues ante una crecida de los tipos de interés. Como consecuencia de las diferencias de composición entre activo y pasivo la empresa B presenta una brecha contraria a la de la empresa A; Tal que:

[4] Duración como principal actor para reflejar el riesgo para con los tipos de interés, ya que indica el tiempo de exposición de estos de las deudas y los activos, reflejándose así también sus diferentes exposiciones. Su justificación se encuentra en el Anexo 2. (Saunders & Cornett, 2019)

$$Da - kDp > 0$$

Indistintamente la empresa B podría cubrirse del riesgo de exposición a cambios del tipo de interés transformando la posición corta de tipo variable de sus pasivos en un tipo de interés fijo de deuda que se asemeje más a la fisionomía a largo del activo. Por ejemplo, una emisión de obligaciones al 10,5%, para el caso, con una madurez similar al proyecto de inversión del activo. Pero igual que A, con ello reduciría su exposición al riesgo en cuanto a tiempo de exposición a este, pero aumentaría el nivel de deuda.

Expuesta la situación ideal entre dos partes para hacer un SWAP de tipo de interés, estas han de conseguir llegar a un acuerdo con la consecuente obligación de liquidar los importes a final de año y mientras este se prolongue. Esto puede ser realizado directamente por ambas partes, lo que presenta claras deficiencias y mayores riesgos asociados al impago, con lo que es tradicional la presencia de una entidad financiera que actúe como agente y *broker* entre ambas partes, recibiendo de esta forma un interés[5] por aceptar el riesgo de pago y garantizar la realización efectiva de los *cash flows* pertinentes establecidos en el contrato. Se describe la posible transacción de interés fijo-variable en la siguiente figura:




[5] Se le conoce como *Crédit risk premium*. Dado el riesgo de cada parte, a este se le suma un % en concepto de Premium y se considera la suma de ambos la parte a devengar a la entidad.

Resultando la operación en:

| | Empresa A | Empresa B |
|---|---|---|
| Pagos por capitales ajenos | -10%*100M€ | -(EURIBOR + 2%) * 100M€ |
| Cobros por acuerdo *SWAP* | 11%*100M€ | (EURIBOR + 3%) * 100M€ |
| Pagos por acuerdo *SWAP* | -(EURIBOR + 3%) * 100M€ | -11% * 100M€ |
| *Cash flow* resultante | -(EURIBOR + 2%) * 100M€ | -10% * 100M€ |
| Posición variable ofrecida por el mercado | EURIBOR + 2,5% | |
| Posición fija ofrecida por el mercado | | 10,5% |

Como resultado de la operación *SWAP,* ha transformado su posición obligacionista fija en un pasivo variable en sintonía con el tipo variable de sus activos y por tanto potenciales rendimientos. Es más, la empresa A si quisiese ir al mercado para cubrir su riesgo, hubiese obtenido obligaciones indexadas al tipo variable EURIBOR + 2,5% (ahorra con el *SWAP* un 0,5%). Del mismo modo, la empresa B ha transformado la posición variable de sus obligaciones en una fija al 10%. Si hubiese acudido al mercado, la empresa B habría pagado 10,5%, lo que le supone un ahorro de 0,5% gracias al contrato *SWAP*. (Saunders & Cornett, 2019)

Ha de ser notorio para el lector que la participación de una entidad mediadora entre ambas que interacciona en su lugar dada la falta de confianza existente y absorbe el riesgo inherente a la operación, a cambio de un interés por el servicio, resulta en claras deficiencias temporales y en pérdida económica traducida en un menos ahorro para las partes. Debería ser de estudio cambio de bienestar que dicha mediación provoca, y si esta desemboca en una preferencia hacia modificaciones de balance en lugar de mercado.

## 3. Smart Contracts. Descripción

El origen de los Smart Contracts es incluso anterior a la introducción del Bitcoin. Nos situamos en la época de la revolución de datos de los 90', cuando Nick Szabo hizo referencia al término, junto a la necesidad inherente de un sistema de computación autónomo capaz de interpretar todo tipo de lenguaje que cree relación entre individuos de forma autónoma. (Szabo, 1997). Pero hablamos de una época donde ninguno podía imaginar aún la existencia de una tecnología pública, segura y a la vez distribuida. Es por esa razón que con la introducción de la tecnología blockchain, los Smart Contracts fueron rápidamente una realidad. (Kehrli, 2016)

El Smart Contract solo se puede entender en un contexto de Blockhain dada su capacidad para registrar cualquier tipo de valor, otorgar confianza para que este sea más eficiente que los tradicionales en el mercado en cuanto a tiempo y coste económico y seguridad dado que una vez este es registrado a la cadena se distribuye de forma descentralizada. (Buterin, 2014)

Para el ejemplo del SWAP, un Smart Contract sería un acuerdo entre partes, pueden ser estas más de dos, firmadas de manera digital. Un tercer agente, un desarrollador de software, puede codificar y ejecutar el código del mismo cuando se produzca el entendimiento entre dichas partes por una cantidad muy inferior al *premium credit risk* derivado de la participación tradicional de las entidades financieras. (Saunders & Cornett, 2019). El código registrado en él exento de errores y sin lugar a interpretaciones, se deriva una confianza en su ejecución automática y en su resultado o *output*.

Con lo expuesto anteriormente el lector sabe que la tecnología Blockhain permite la ausencia de terceras partes mediadoras traduciéndose en eficiencias de tiempo y dinero para las partes. Con lo que los Smart Contracts basados en una red Blockhain se da el siguiente paso, la automatización de acciones contractuales de forma distribuida. (Kehrli, 2016) (Buterin, 2014). Se le derivan los siguientes beneficios:

**Rapidez y actualizaciones en tiempo real:** La sustitución de la que solía ser una actividad humana, es reemplazada por un sistema de actualización automático.

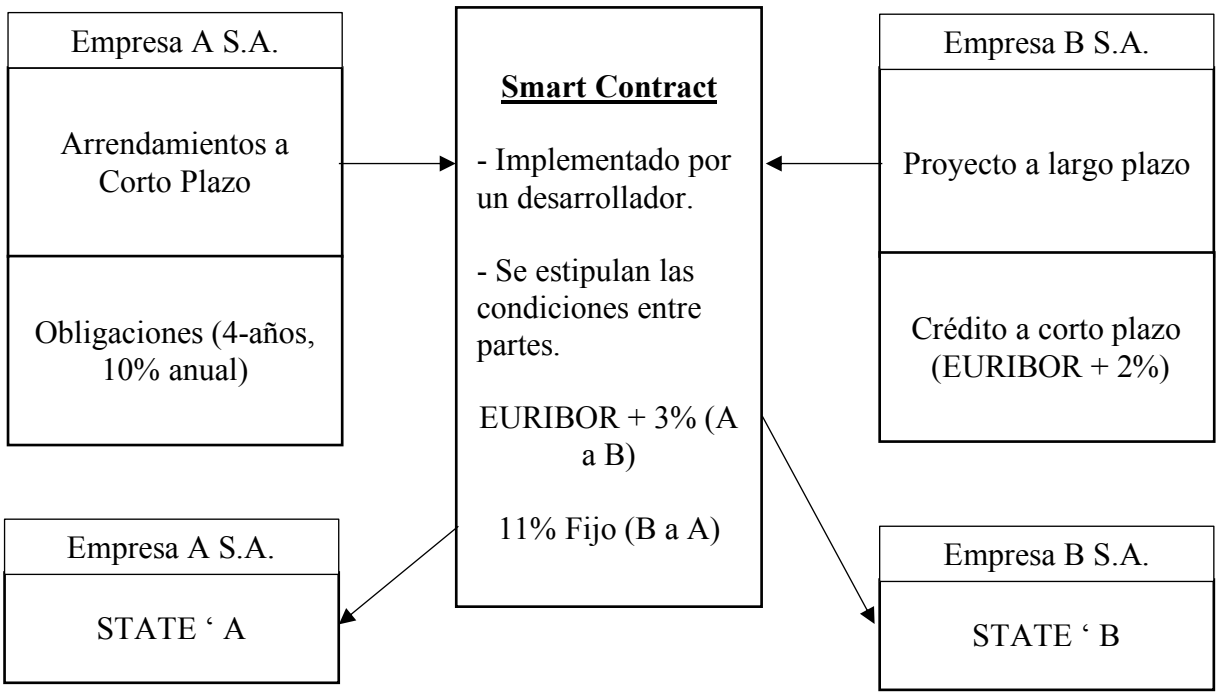
**Precisión:** Las transacciones no serán solo automáticas, sino expuestas a menor error por la inexistencia de la figura humana de por medio.

**Menor riesgos:** Con el proceso de ejecución virtual de los contratos se eliminan posibles manipulaciones o incumplimientos debido a que es regulado por código distribuido por la red y no depende solo de un individuo.

**Menos intermediarios:** Si bien es cierto que se precisa de la acción de un desarrollador, este no implica pérdidas en eficiencias y su acción tiene un valor sensiblemente menor a la presencia de un tercer agente tradicional.

**Menor coste:** En la línea de lo anterior, la no presencia de agentes intermediarios tradicionales se traduce en un menor coste para las partes. (Kehrli, 2016)

Siguiendo el ejemplo anterior del SWAP, ahora se analiza que partes debería recoger en forma de código un Smart Contract:




## 4. Como funcionan los Smart Contracts

**Código:** Lo que se escribe dentro de un Smart Contract.

Es muy importante que los Smart Contracts sean un reflejo fiel de lo que las partes quieren conseguir con el contrato. Su funcionalidad se asemeja a la de un programa de ordenador cualquiera al que se dota de las condiciones y se le definen estadios susceptibles futuros. La participación humana es importante en este proceso de automatización, dado que se han de prever sucesos para que el resultado de la ejecución sea válido o incluso realista.

**Registro Distribuido:** Como se hacen efectivos o son publicados los Smart Contracts.

Cuando un código es escrito de manera que relata las condiciones de las partes y estas así lo verifican, se le otorga una llave privada criptográfica para que sea incluida en el monto de transacciones que recoge el bloque en curso. Esto puede ser llevado a cabo gracias a las ventajas que de la Blockhain se derivan. Se trata pues un Smart Contract como una transacción de valor dinámica en el tiempo.

**Ejecución:** Como el contrato es procesado.

Una vez se valida el bloque y por tanto el contrato es añadido al registro distribuido, todos aceptan los *outputs* que de su ejecución se derivan. La red, entonces, actualiza los datos para su constancia y se valida el cumplimiento por parte de todos los participantes de la misma de que el Smart Contract se ha llevado a cabo satisfactoriamente y sin dejar lugar a dudas. En este tipo de movimientos la responsabilidad de aceptación o rechazo de los outputs no recae sobre un único individuo, por lo que manipulaciones y fraudes son reducidos en su totalidad. (Kehrli, 2016)


Figura 7: Aspecto de un Smart Contract. Elaboración propia

## 5. Oracle: La plataforma *cloud* distribuida

Las plataformas que permiten la ejecución de Smart Contracts interactúan con el mundo real para obtener información necesaria y actualizar los valores de *output* de los contratos en vigor. Se precisa, así de la participación de código que permita al contrato enlazar o hacer referencia a webs *API* para así obtener información de otros sitios fura incluso de la plataforma. Dado que en la red no hay seguridad ante la información que se recibe, el contrato ha de ser capaz de obtener la información de webs establecidas como seguras o *Oracle*. (Solomon, 2018)

Oracle se entiende como una fuente de información externa a la red en la que las partes confían para representar la realidad de la información. Un Oracle puede ser definido de distintas formas según las partes prefieran:

- Asignación por preferencias de consenso entre las partes afectadas por el contrato.

- Usando un servicio Oracle descentralizado, externo a la red, donde se recoge toda la información de forma que esta se registra como única y veraz. Es el caso de *Oraclize,* una red blockchain que actúa de mediador entre el Smart Contract y la web *API* en caso de que así lo prefieran las partes. (Kehrli, 2016)

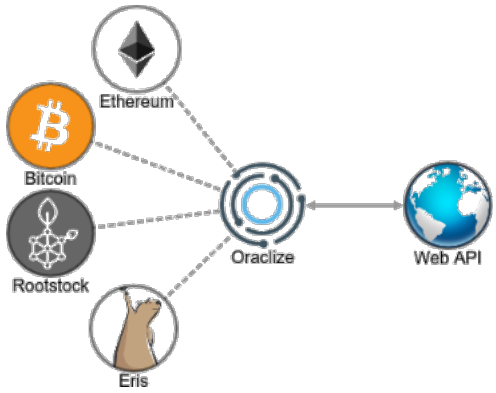
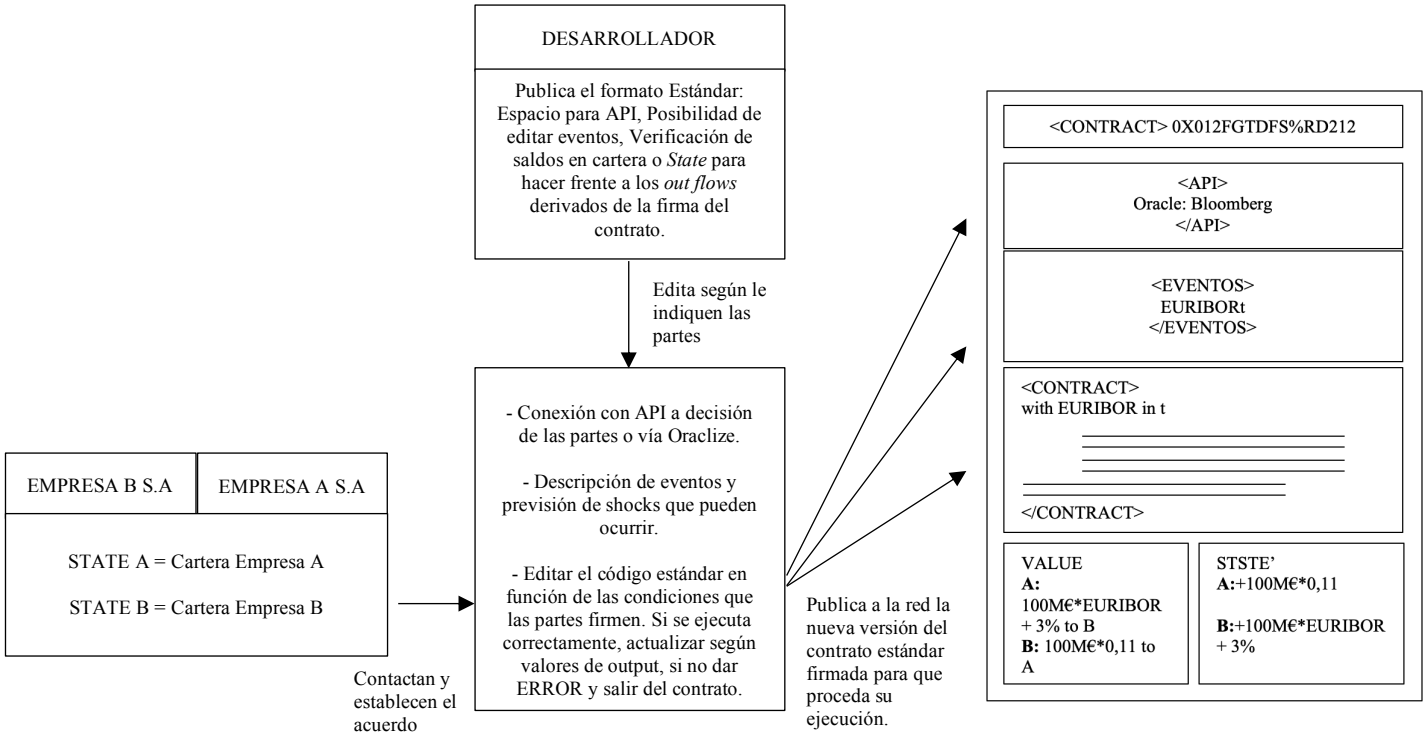



Figura 8: Ilustración función plataforma *Oraclize*

Por lo tanto, siguiendo lo que se comentaba anteriormente que el código, previamente definido, era leído y ejecutado, los resultados pueden variar con el tiempo y/o con la información que se reciba de forma externa del web *API* de definido como fuente de confianza. (Solomon, 2018)

Para el ejemplo, basado en el tiempo (t) de ejecución y de información ajena a la cadena, sería necesaria la aparición de una web API de consenso entre partes, y en su defecto la participación de *Oraclize* (Kehrli, 2016). Es por eso que a continuación se presentan todos los actores que participarían en el proceso de ejecución de el Smart Contract del SWAP de tipo de interés, siguiendo este el modelo de la figura 7:




Con ello las partes consiguen realizar una actividad comercial fruto de la necesidad de cambiar su posición ante posibles variaciones del tipo de interés afecto a sus activos y pasivos con un Smart Contract estableciendo la confianza necesaria para su éxito. Beneficios claros se derivan de esta, como su ejecución casi inmediata y una menor pérdida de ahorro potencial que de esta su aplicación se deriva.

Con la evolución hacia la tecnología Blockhain 2.0 se crea una disyuntiva clara entre aquellas que posibilitan un espacio para el desarrollo y la ejecución de los Smart Contracts y las que no. Bitcoin, por ejemplo, es una red ideal para las transacciones de criptomonedas Bitcoin, pero de otro lado posee una capacidad de codificación limitada a la simple lógica de transacción tradicional. (Kehrli, 2016).

La plataforma *Ethereum*, en cambio, es la plataforma Blockhain pública más avanzada para la ejecución de Smart Contracts a día de hoy. Con un sistema *Turning-complete* en su red capaz de identificar y ejecutar cualquier código que se registre. (Buterin, 2014). Los Smart Contracts, así, pueden ser dotados de cualquier tipo de código y ser registrado en la red sin excepción. Ethereum, se mantiene gracias al sistema PoW de una red pública. Las transacciones son realizadas aceptados con su propia criptomoneda o *token*, en este caso *Ether*, *ETH* o gas a modo de incentivos aceptados por la red para la actividad de los mineros y desarrolladores. (Kehrli, 2016)

## 6. Ethereum.

*"Ethereum: A next genereation Smart contract and decentralized application Platform"*. Bajo este título se presentaba la plataforma Ethereum. Un espacio totalmente innovador, lleno de posibilidades como el desarrollo de aplicaciones distribuidas y los Smart Contracts, basado en la tecnología Blockhain que la precede y pública. (Buterin, 2014)

Si bien fueron pocos los que vieron la grandeza de Bitcoin más allá de sus posibilidades especulativas, Vitalik Buterin fue una de esas mentes que las generaciones modernas tardarán en olvidar porque supo adaptar las oportunidades que ofrecía la tecnología Blockhain a las necesidades de la sociedad para idear la plataforma Ethereum. (Buterin, 2014). Siempre interesado en el mundo que se abría con la introducción de la primera criptomoneda, entró a formar parte de este mundo con sus participaciones en blogs y artículos en la "Bitcoin Magazine" de la cual es co-fundador. Nos situamos en 2011, cuando la red de Bitcoin registraba una media de 2.000 trans/día, lejos de las más de 280.000 trans/día en el momento de escribir. (blockchain .com). Muy lejos, por tanto, de causar impacto real, pero sí cerca de generar interés.

El acontecimiento clave tuvo lugar en 2014, cuando después de abandonar su trayectoria como divulgador de la tecnología, Vitalik Buterin decide desarrollar, junto a un grupo de personas, un proyecto de ambiciones más allá de lo material y pasar así a la historia de la tecnología blockchain. El proyecto recibió el nombre de Ethereum (Kehrli, 2016) y con él se hacía posible la ejecución de cualquier código en una misma plataforma pública, segura y de forma distribuida, dando así respuesta, a la necesidad que en los 90 Nick Szabo apuntó era necesario para poner en circulación los Smart Contracts.

Ethereum es, entonces, una plataforma programable, pública y distribuida. En esencia un espacio alternativo para la creación y desarrollo de aplicaciones descentralizadas basado en la tecnología blockchain, capaz de interpretar y ejecutar cualquier código que se le defina. Sea en el lenguaje que sea (C, C++, JavaScript, Python…), (Kehrli, 2016) ,lo que se califica como *Turning-complete programming language*. Esto se traduce en un espació idóneo para cualquier desarrollador que desee crear una aplicación de forma distribuida en toda la red y que a su vez elimine el poder centralizador de otras. (p. ej. Apuestas deportivas en Ethereum). (Mattila, 2016)

La gran diferencia entre Bitcoin y Ethereum, salvando diferencias estructurales más allá del objetivo del trabajo, es que, la primera tiene grandes limitaciones con lo que interpretación de código representa, por tanto, se califica de *Turning Incomplete programming language*. Unas limitaciones que no se tradujeron en ineficiencias dado el segmento de mercado que cubre, pero

de funcionalidad estática. Bitcoin tarda una media de 3 días en validar y hacer efectiva una transacción, y dado que el valor de su token varía según el mercado, este cambia en el tiempo provocando así que el valor de 1 BTC en n ≠ 1 BTC en n+1.

Ethereum quiere adaptarse a las necesidades y limitaciones humanas haciéndose accesible a toda la sociedad con protocolos sencillos y abiertos a modificación por parte de los usuarios, si esta su aportación sigue esa sencillez que defiende y solo si prueban servir para mejorar ineficiencias. Quieren ser espacios modulables, sin que esto signifique la creación de burbujas privadas en la red, junto a un proceso ágil de aplicación y modificación de códigos abierto a todo aquel que decida desarrollar su idea de aplicación. (Buterin, 2014)

### 6.1 *Ether*

Las monedas digitales o tokens para Ethereum son los llamados *Ether*, *ETH* o gas. El *ETH* es la criptomoneda aceptada por su red. Los desarrolladores han de consumir Ether para habilitar o editar Smart Contracts publicados en la plataforma y los usuarios deben gastar Ether para percibir las transacciones de las distintas aplicaciones. Las transacciones que resulten como no válidas o que no tengan suficiente *ETH* se desestimarán del mismo modo que lo hace la red Bitcoin. (Kehrli, 2016)

La *Ethereum Virtual Machine* es un ordenador universal por la característica *Turning complete* que permite la ejecución de cualquier código en la red Ethereum. Los desarrolladores son compensados por su labor de dotar de lógica a un Smart Contract y según su complejidad serán compensados con mas o menos *ETH* en forma de interés por el servicio a las partes. Por otro lado, los mineros, que pueden también ser desarrolladores, son incentivados por cada bloque que añaden a la red con una cantidad de *ETH* según su complejidad. (Frantz, 2016) (Kehrli, 2016)

### 6.2 *Cuentas Ethereum*

En la línea de lo que Bitcoin propone con sus carteras o *wallets*, como si de cuentas de banco se tratara, Ethereum lo adopta y lo denomina cuentas o *accounts* divididas en dos grandes grupos:

> **Cuentas de almacenamiento de *ETH*:** Las que se asemejan más a las wallets de Bitcoin. Se denominan *External Owned Accounts, EOA*. Uno puede hacer movimientos de cartera con ella usando la criptografía asimétrica característica de una blockchain. Por lo que recoge la capacidad de transacciones de la blockchain 1.0 donde el *state* inicial hará referencia a la *EOA* del individuo. (Buterin, 2014) (Frantz, 2016)

**Cuentas de almacenamiento de *ETH* y código**: Denominadas *Contract Accounts* son activadas cada vez que les es enviada o transferida una cantidad de ETH en ellas, permitiendo así que su código pueda ser leído, modificado y enviado para su ejecución. (Frantz, 2016) (Kehrli, 2016). Se emiten a la red para su adhesión al grupo TX del *transfer counters* de igual forma como si de una simple transacción se tratara, pero siendo su afectación dinámica a las condiciones denominadas en el código.

De acuerdo con lo que dictamina Jerome Kehrli, los Smart Contracts en Ethereum no han de interpretarse como un código estándar, sino uno adaptable y modificable, y no como inteligencia artificial, sino todo lo contrario, automatismos que precisan de la participación humana.

### 6.3 *El precio del Gas o ETH*

Siendo el *ETH* o gas la llave de acceso a los Smart Contracts de la red Ethereum y este valorado a precio de mercado. Se puede decir que cada Smart Contract tendrá un precio ligado a la dificultad de codificación, las condiciones del mismo, previsión de escenarios futuros y el número de API que esta su ejecución precise.

El coste de emisión de un contrato es decisión del usuario, y el desarrollador puede estar de acuerdo o rechazar la oferta hasta que se llega a un acuerdo. La efectividad y realidad de los *outputs* dependerán del trabajo de los desarrolladores o de los mineros. Aquí tiene un papel importante la relación oferta y la demanda de individuos capacitados para la tarea, no del precio de mercado del *ETH*.

Para hacer efectiva la transacción, los intercambios de valores o simplemente obtener los outputs del código de los contratos, una parte de gas es consumida en el proceso. Todo lo anterior se ha de prever de antemano porque de lo contrario el contrato no se ejecutará correctamente. Si resta algo de *ETH* en el Contrato una vez liquidado, esta es automáticamente transferida al desarrollador.

La razón de que la edición, publicación, ejecución y resultado genere un gasto, es un método de prevención ante bucles infinitos en los contratos considerados como fraude por parte del desarrollador que edita el código. (Kehrli, 2016)

## 7. Las diferencias entre Bitcoin y Ethereum.

Referenciado a los conceptos del apartado III, se sigue con la exposición de las principales diferencias entre las plataformas Bitcoin y Ethereum.

**Registro de bloques**

Ethereum registra bloques en su cadena cada 13,5 segundos, Bitcoin lo hace cada 10 minutos de media. Por lo tanto, si se realiza una transacción en cada una de las redes al mimo tiempo, la de Ethereum se haría líquida antes que la de Bitcoin. (blockchain .com) (Etherchain.org). Si bien lo anterior es cierto, cabe destacar que, aunque el protocolo de validación y de consenso sea el mismo, el PoW, para la red Bitcoin una transferencia después de ser añadida a un bloque y este ser aceptado por la red no se hará efectiva hasta que cierto número *z* de bloques sean añadidos con posterioridad para así, descartar cualquier ataque en la información de la red.

Un menor tiempo de generación entre bloques se traduce en el incremento de la probabilidad de que aparezcan bloques huérfanos y más *forks* creadas. Ethereum asumió ese riesgo y redujo sensiblemente el tiempo de generación de bloques, pero a diferencia de las *forks* que aparecen en Bitcoin, ésta incentiva el trabajo de los mineros a encontrar la referencia de la *fork* creada con la cadena principal. Son los llamados *uncle blocks* (Zheng Z. X., 2018)

**Recompensa por bloque.**

La plataforma Ethereum devenga al día 15.000 *ETH* en forma de recompensa por encontrar un total de 6.400 bloques, lo que resulta en un incentivo de 2,34 *ETH* por bloque. La capacidad de retorno para la minería en Ethereum persigue la máxima de no generar más de 18 M ETH al año para evitar una inflación de su valor, semejante a la de un sistema monetario actual. (Etherchain.org)

El número de tokens como incentivo a la resolución del algoritmo y encontrar el valor hash de un bloque en la red Bitcoin es de 6,25 BTC y un máximo de tokens en el mercado con límite a 21 M BTC. (blockchain .com)

**Recompensa por un *Uncle Block***

En las plataformas Blockhain algunos bloques son encontrados más tarde y no forman parte de la cadena. Para la de Bitcoin esos eran denominados huérfanos o *orphans* y son automáticamente desestimados. En la red Ethereum son denominados *uncle* y pueden ser referenciados más adelante a la cadena principal. (Kehrli, 2016). La *uncle reward*

por encontrar la unión entre un bloque que no pertenece a la cadena, cuando en realidad así debería ser, se cifra en 1,49 ETH. (Etherchain.org)

Esto permite incentivar el trabajo computacional de un minero, aunque exista una gran posibilidad de que, si consigue verificar un bloque, este no pertenezca a la cadena principal y resulte ser un *uncle*. El máximo de *uncle blocks* que la red permite referenciar por bloque añadido a la cadena principal es de 2. (Kehrli, 2016) Una vez llegadas esas 2 referencias, se abandonan todos los trabajos computacionales para aquellos denominados, ahora sí, huérfanos y trabajar para añadir en la cadena principal.

**Tamaño de los bloques.**

En este momento el tamaño medio de un bloque Bitcoin es de 1,2 MB, mientras que Ethereum consigue un sistema innovador de referenciado a las transacciones denominado *Patricia Tree* que resulta en mayores eficiencias de espacio. (Buterin, 2014). Registran 26 KB de espacio ocupado de media por bloque. En la actualidad un bloque Bitcoin permite registrar una media de 2.500 transacciones. (blockchain .com) Con Ethereum es distinto dado que no existe un número de transacciones finitas, sino que existe un máximo de gas a almacenar por bloque. Actualmente es de alrededor de 9.500.000 de *ETH*. (Etherchain.org).

# V. TECNOLOGÍA BLOCKCHAIN: APLICACIONES

## 1. El impacto de los Smart Contracts.

Con la tecnología Blockhain la posibilidad de prescindir de los servicios financieros parece ser real. No estando conforme con eliminar la mediación de los bancos en las transacciones, con la realidad de los Smart Contracts y los *Autonomus agents,* las actividades financieras tradicionales se ven, si cabe, aún más afectadas, y se plantea un escenario en el que prácticamente todas ellas pueden ser realizadas de forma descentralizada *peer to peer*. Son ejemplos: *Trading* y especulación, devengo de cupones o dividendos por tenencia de acciones, la firma de hipotecas, el *crowdfunding* entre empresa o establecer pólizas o rentas de seguros, entre muchas otras. Todas ellas pueden ser ejecutadas gracias a la capacidad de creación de aplicaciones de forma distribuida de Ethereum y la ejecución de Smart Contracts. (Kehrli, 2016) (Tapscott, 2016)

Se hace evidente una remodelación necesaria a gran escala del sector financiero para adaptarse a la nueva situación. Cabe destacar que empresas del sector de la banca, como podría ser El Banco Santander, ya trabaja en un sistema de red Blockhain de forma privada, en el cual solo sus clientes podrán manejar datos, y otros pocos, los empleados/as, podrán validarlos. Este caso particular del banco Santander prueba la capacidad de adaptación de las entidades financieras al nuevo escenario tecnológico, pero difiere en los objetivos que persigue Nakamoto. (Mattila, 2016) . Se hablará de esto más adelante en el apartado VI.

Igual que el banco Santander, que para el ejemplo es uno de los que está testando las posibilidades que de la tecnología se derivan, hay muchos otros reacios a pensar que su institución va a perder fuerza de una forma exponencial a la medida que la tecnología Blockhain se vaya actualizando. Pero la evolución de las transacciones de Bitcoin a la plataforma distribuida Ethereum es tal que ya se ven cambios en sectores ajenos al financiero, traduciéndose estos proyectos reales o en fases de desarrollo avanzadas. (Tapscott, 2016)

Los siguientes son sectores que presentan a día de hoy intención de adoptar o implementación real de un modelo basado en red Blockhain:

Turismo


Uno de los sectores interesantes a investigar y susceptibles de usar en un futuro no muy lejano tecnología Blockhain adherida a una red *Turning complete* para poder ejecutar Smart Contracts,

es el turismo. Airbnb, para el ejemplo, es una plataforma con nombre, novedosa y con actividad en más de 192 países, encuentra su razón social en el alquiler de alojamientos donde los usuarios publican en la misma la disposición de un inmueble para que este sea susceptible de ser alquilado para una estancia pasajera y de muy corta durada. Airbnb operado por una plataforma blockchain podría generar sinergias instantáneas para la empresa, ya que podría verificar la realidad del inmueble publicado en su página web, validar la información proporcionada por las partes interesadas y, por último, vía un Smart Contract cerrar la operación entre ambos haciendo constar, y sin lugar a dudas, la propiedad real para el periodo de tiempo establecido del servicio de alojamiento. Con ello Airbnb reduciría el tiempo de verificación de identidad y propiedad tanto del emisor como del receptor, evitando así un gran número de insatisfacciones que pueden surgir de ambas partes. A día de hoy la plataforma da garantías de servicio atendiendo la opinión de clientes anteriores, dejando que estos puntúen al propietario/a ofertante del servicio y permitiendo un espacio para que el cliente deje su *feed-back*.

Votaciones y procesos electorales

A modo de ejemplificación de un proceso de transición hacia una democracia transparente se presenta un mecanismo basado en emisión de Smart Contracts para que cada individuo pueda registrar su voto en un proceso electoral. Precisa de una red que enlace cada uno de los Smart Contracts que se registren, haciendo así uno referencia al siguiente una vez se ha tenido en consideración la participación del anterior. Con unas consideraciones, dadas las condiciones que se han de tener en cuenta en forma de código, como serían la necesidad de que el individuo este registrado en el censo, tener la edad para ejercer el derecho, limitar el número de votos a uno por individuo y marcar un tiempo límite de emisión de votos en forma de contratos a la red. Todo lo anterior recogido en una última línea de código que registre el voto que se deriva de la ejecución del contrato, junto a los anteriores y dejar paso al siguiente para que una vez haya ejecutado su código registre el voto resultante, y así consecutivamente hasta que no existan más contratos calificados como admitidos por haberlo hecho en el tiempo estipulado. Si bien pueden existir casuísticas, la participación del código y su adaptabilidad permite al individuo recoger su situación y expresarla en forma de eventos. Por ejemplo, si alguien reside en el extranjero, pero quiere ser partícipe de las elecciones del país de origen, podría hacer constar su casuística en forma de eventos para evitar posibles errores en le ejecución. Con este método uno sabe con certeza que los resultados son los únicos representativos de la realidad, dado que no pueden ser en ningún caso modificados, se eliminan los votos nulos y, por supuesto, se generan eficiencias en forma de tiempo para la emisión y recuento de votos junto a un menor despliegue de efectivos para la realización del proceso electoral, que se traduce en menores costes. (Frantz, 2016)

Con lo anterior se deja constancia que cualquier proceso que precise de votación distinto a uno electoral, puede ser susceptible de transición. Solo se ha de adaptar el contrato a las condiciones que el voto o el proceso de votación requiera. Por ejemplo, votación en una junta de accionistas.

Información Personal

¿Como o cuánto cuesta los gustos, tradiciones, inquietudes, actividades o incluso la dirección de hogar de un individuo? Esta es una pregunta que con el auge de la web 2.0 junto a Internet se hicieron las grandes corporaciones. Se dieron cuenta que para poder segmentar el mercado y adaptar su negocio a las necesidades del consumidor era de vital importancia tener acceso a cuantos más datos sobre los individuos, mejor. Empezó así una guerra entre las empresas para conocer al máximo a sus clientes e incitar así a la compra segmentada e individualizada. Facebook, Twitter, Instagram y Google son ejemplo de corporaciones que parte de su razón social implica la cesión de datos individuales y personales. Esta información sensible gestionada por entidades centralizadas como las anteriores se encuentra en el punto de mira. La red Blockhain se presenta como alternativa viable por lo que a registro y gestión de dichos datos representa. Con ella el individuo podría registrar su información relevante para las empresas, y para que las mismas puedan tener acceso a ellas han de desembolsar la cantidad que la red estime se valora dicha información y generar un Smart Contract donde figure la propiedad de la información en todo momento. Con esto se elimina cualquier posible fraude y se permite así una gestión a título personal de la información de uno mismo. (Xiao, 2020) (Zheng Z. X., 2018)

*Internet of Things* (IoT)

Desde el comienzo de la red Blockhain con el lanzamiento de Bitcoin en 2008 los casos reales de uso de la tecnología han ido incrementando y se ha ido expandiendo a medida que la misma ha ido evolucionando. Muchos campos se han visto afectados de forma directa o indirecta de la suplantación que esta revolución supone, como es el caso del sector financiero, pero hay otros que con la nueva tecnología han visto una oportunidad de crecer. Es el caso del IoT. En la actualidad muchos sectores, tanto privados como públicos están empezando a comprender la grandeza de la tecnología Blockhain e intentan adaptarse a ella. Con estos procesos evolutivos, el IoT es cada vez más una realidad, y la Blockhain parece ser la última pieza restante del puzle. Se entiende IoT como la capacidad de relación entre dispositivos de cualquier tipo de forma sincronizada y totalmente automatizada a través de Internet. Con una red blockchain la plataforma que encabara la relación entre dispositivos a través de Internet, podría reconocer la propiedad e permitiría la interactuación que el IoT precisa.

Ethereum, dada su característica *turning complete* parte como favorita para emplazarla. (Pilkington, 2016) (Zheng Z. X., 2018)

IBM Blockchain *Platform*

IBM es una empresa multinacional que fabrica y comercializa *hardware* y *software* para ordenadores, y ofrece otros servicios de infraestructura, alojamiento de internet y consultoría en una amplia gama de áreas relacionadas con la misma informática. Cuenta con una cartera de clientes líderes dentro de los sectores como financiero, aerolíneas, manufacturas y distribuidoras de productos de consumo.

La compañía sigue la filosofía de hacer ganar a sus clientes ventajas competitivas con sus productos o servicios para que estos les permitan alcanzar sus metas de cuota de mercado, y para conseguirlo, IBM ha hecho una clara apuesta por la tecnología Blockhain. IBM ha implementado una red de características que se asemejan a la del banco Santander por su característica *permissioned,* pero desarrollada de manera que esta se asemeje a las características *turning complete* de Ethereum. Consiguen así un servicio blockchain capaz de adaptarse a las necesidades del cliente permitiendo que este haga uso de la misma para interactuar con otros usuarios. (Pilkington, 2016). Consiguen así incrementar la veracidad y la transparencia de tanto clientes como proveedores adheridos a la red, al mismo tiempo que crean una nueva forma para los clientes de intercambiar datos entre si. En la actualidad IBM tiene registrados 500 proyectos con sus clientes, con más de 85 redes blockchain propias que transforman la cadena de aprovisionamiento, entregas y financiamiento globalizado. Son ejemplos de proyectos los siguientes:

**IBM Food Trust - Walmart**

El trabajo realizado por la compañía Walmart e IBM, impulsado por el servicio Blockhain de IBM, resulta en una red de distribución más segura y confiable para el consumidor final. Con el sistema tradicional si se desea saber que productos son susceptibles de presentar errores significa que se ha de hacer una búsqueda intensiva para encontrarlos, mientras que con el proyecto Food Trust se habilita la conectividad entre productor, procesador, distribuidor y minorista para que estos compartan un seguimiento exhaustivo del producto que resulta en eficiencias de tiempo, ya que se sabe en todo momento cuales son los potenciales productos en riesgo. Esto permite a los minoristas conocer mejor los productos, lo que se traduce en un valor añadido para el cliente. (IBM, 2019)

**Maersk.**

El gigante de la logística usa el servicio de red Blockhain de IBM para crear el concepto TradeLens el cual incentiva las conexiones entre las partes participantes de un proceso de entrega. Con ello, el proyecto Maersk consigue ganar en tiempo y costes tanto para el cliente final, como para la empresa misma. (IBM, 2019)

**Smart Dubai.**

Dubai quiere llegar a ser la primera *Smart City*, y quiere conseguirlo de la mano de los servicios blockchain de IBM. El servicio Dubai Blockchain Platform pretende hacer más accesible la tecnología al gobierno de Dubai y a las empresas privadas para poder liderar la nueva era tecnológica y crear una nueva ola de oportunidades económicas e innovación digital. (IBM, 2019)

# VI. LIMITACIONES DE LA TECNOLOGÍA BLOCKCHAIN

No ha de extrañar al lector que llegados a este punto se pregunte como es posible que, teniendo el método, como son los Smart Contracts, y la plataforma, como podría ser Ethereum, la automatización de los procesos expuestos hasta el momento no esté en la orden del día. La respuesta reside en las características de las redes blockchain públicas o *permissionless*. (Zheng Z. X., 2017)

Una red *permissionless* o pública es aquella que persigue, ante todo la descentralización, como podría ser Bitcoin y Ethereum, pero no son el único tipo de red blockchain que existe. Para dejar constancia de la definición formal, es una blockchain gratuita en la que uno puede entrar y salir tantas veces como dese, siempre que este posea un pseudónimo, cuenta o *public key* que le habilite el poder realizar o recibir transacciones de valor con los miembros de la misma red de forma anónima. La gobernabilidad se entiende de forma pública y distribuida donde cualquiera puede participar del proceso de consenso, si bien, solo los mineros perciben derecho a ejercer voto para el proceso de consenso y en función de su poder computacional aportado, este tendrá más o menos valor. El espacio blockchain público habilita la confianza entre partes con la seguridad que se deriva de sus características criptográficas. (Xiao, 2020)

Con la entrada de la Blockhain 2.0 y las posibilidades que con ella se desprenden, el siguiente paso para la tecnología debe ser el englobar todas las aplicaciones y usuarios de forma no solo descentralizada, sino globalizada. Pero, por desgracia, el conocimiento tecnológico actual, resulta en insuficiencias para llegar a una red pública, distribuida y globalizada capaz de ser accesible por cualquier individuo sin que esta pierda en eficiencia. (Kehrli, 2016)

Dado que la blockchain pública es la única que defiende la descentralización, y como consecuencia, con la única que se puede llegar a un modelo de red globalizado y distribuido, se detallan a continuación las limitaciones y vulnerabilidades del sistema propuesto por Satoshi Nakamoto, que a día de hoy se tratan de solventar:

> **Relación entre rendimiento y seguridad:** El modelo de Nakamoto ha recibido muchas críticas por su rendimiento. Un rendimiento que se mide en *Transactions Per Second* (*TPS*). Estas limitaciones se explican por las implementaciones de seguridad requeridas hasta que esta es añadida a la red. Uno podría decir que, si se redujera el tiempo de creación de un bloque, para el caso de Bitcoin 10 minutos, se conseguirían eficiencias de tiempo y ganar en rendimiento. Si se aumentara pues el número de TPS de la red Bitcoin, sería a de generar mayores *forks,* derrochando así trabajo computacional de mineros honestos.

Si por otro lado se propusiera hacer mayores bloques aumentando su capacidad, aumentando así las TPS potencialmente capaces de ser registradas, pero haría más difícil su propagación por la misma red. Se ha de buscar un equilibrio entre eficiencia y peso del bloque. Para que el lector se haga una idea del nivel de ineficiencia comparado con sistemas centralizados, se habla que Bitcoin realiza 7 TPS, mientras que VISA *payment network* procesa de media 2.500 TPS.

Con la llegada de Ethereum se propone, como se ha expuesto en temas anteriores, remunerar el encontrar la conexión entre un bloque *uncle* con la cadena principal. De este modo se pueden generar bloques en un rango de tiempo menor remunerando el trabajo realizado para encontrar conexiones entre bloques que no forman parte de la cadena principal. Se traduce este en un aumento de la eficiencia en cuánto a TPS, ya que la plataforma Ethereum, de media registra alrededor de 10 TPS. (Xiao, 2020)

**Ineficiencias energéticas:** A mayo 2020, la red Bitcoin consume de media por transacción 572 KWh, o lo que sería lo mismo, el abastecimiento de 20 familias para el mismo día. (Digiconomist.net). Esta cantidad tan grande de energía es necesaria dado el sistema PoW que usa esta misma red y la mayoría de las redes públicas. A medida que la red de Bitcoin ve incrementada su comunidad de mineros, el protocolo de consenso propuesto por Nakamoto ha de modificarse para aumentar la dificultad del algoritmo y así conseguir mantener los 10 minutos de generación entre bloques, lo que a su vez provoca que sus mismos mineros inviertan en más y mejores equipos informáticos para encontrar de forma más rápida el hash, y así no perder posición dado este incremento de dificultad. Es un ciclo vicioso que no hace más que incrementar a medida que la red gana protagonismo. En respuesta a este problema, la comunidad blockchain ha puesto sobre la mesa procesos alternativos al PoW, como el *Proof. of Stake (PoS)*[6]. (Xiao, 2020)

Ethereum a día de hoy sigue el consenso según lo estipula Nakamoto, si bien introduce cambios importantes en la anatomía de los bloques, concretamente en el sistema *Markle Tree*, que el lector lo recordará del apartado III. Modifica la forma en la que se almacenan y se registran las transacciones de valor en el mismo y en el como se gravan en el bloque. El sistema recibe el nombre de *Patricia Tree*. (Buterin, 2014). De este modo Ethereum consigue repercutir un gasto de 24 KWh de media por transacción. Ha de estar en conocimiento del lector que Ethereum propondrá una remodelación del sistema de consenso en un futuro cercano para así responder a un sistema PoS, mucho

[6] *Proof of Stake (PoS)*: Alternativa considerada energéticamente más eficiente que el PoW. Un *stake* se refiere a las monedas o tokens de propiedad individual, subyacentes al poder computacional del minero. En el proceso de consenso, la importancia del voto es ponderado al nivel de *stake* de los mineros.

más escalable que el actual PoW. Lejos aún de la eficiencia de redes centralizadas como la de VISA. (Digiconomist.net). (figura 9)

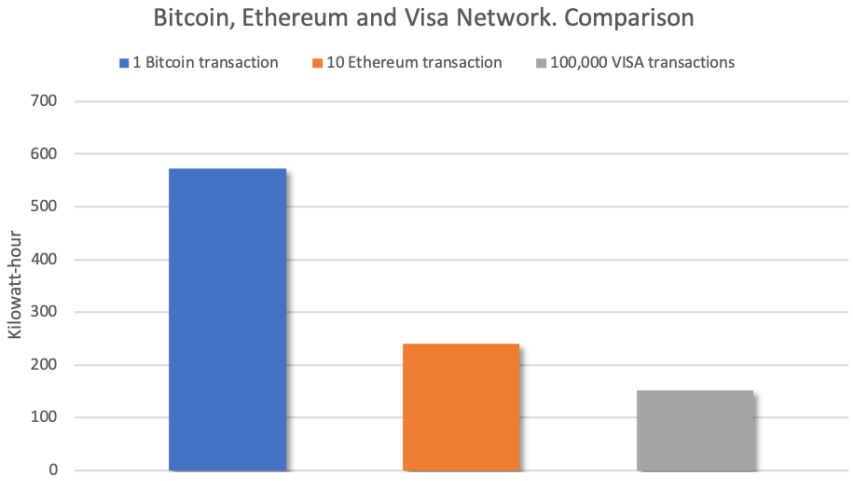



Figura 9: Comparativa gasto energético Bitcoin, Ethereum y VISA. Elaboración propia. Datos: Digiconomist

**Minería egoísta:** El problema conocido como *Selfish Minning* existe debido a que con el 51% de consenso de la red un bloque es añadido a la cadena principal, entonces se sobreentiende ese bloque el único representativo de la realidad y confiable para el resto. El sistema de consenso PoW asume el riesgo de tener centralizado el poder minero y lo controla con las remuneraciones por encontrar bloques. La capacidad de representación que un minero tiene en una red de consenso PoW viene determinado por su productividad, por lo tanto, su número de bloques encontrados. (Xiao, 2020). Un grupo de mineros, en el supuesto que estos representen el 51% del poder de computación y creen una alianza podrían ocultar los últimos bloques minados y publicarlos de forma estratégica para su beneficio y despreciar así el trabajo hecho por los nodos honestos propiciando así el problema *Double Spending*. Aquí reside la clave para entender la existencia de los *halving* en la red Bitcoin, dado que con ellos se desincentiva el tener mayor concentración de poder computacional. A mayor poder computacional, mayor coste para el minero grande que ve como el *halving* le impide recuperar su inversión. Nakamoto ya predijo este escenario era posible, y por eso la emisión de Bitcoin en el mercado está definida con un máximo de 21 M. A día de hoy hay 18.4 M *outstanding*. En la actualidad se puede decir con seguridad que solo han sido objeto de ataques redes pequeñas como fue el caso de *Monacion*, pero nunca a Bitcoin u otra red Blockhain dominante.

Vitalik Buterin rediseña el modelo de *hash rate* que propone Nakamoto con el algoritmo *SHA-256*, calificándolo de vulnerable ante posibles burbujas de mineros dentro de la misma red. Así Ethereum sigue con el mismo sistema de generar un hash que junte el bloque con el resto de la red, pero no de forma aleatoria, sino basado en información de la misma cadena. El algoritmo que usa Ethereum para encontrar el Hash del bloque se basa en información de los *State* de forma aleatoria, tener en cuenta información criptográfica de unas transacciones en N de forma aleatoria y obtener así el hash del nuevo bloque. (Pilkington, 2016). De este modo se permite a los Smart Contracts registrar cualquier tipo de código y se precisa de toda la información de la misma red para encontrar el *hash values*, con lo que se desincentiva el controlar el 51% de la red y publicar bloques para un interés. El modelo desincentiva así la creación de alianzas entre mineros, pero no prevé su formación.

**Burbujas de mineros y centralización del riesgo:** Dado el sistema de incentivos para con la minería en el proceso de consenso de Nakamoto, la recompensa es mayor, cuánto mayor sea tu poder computacional. De este mismo modo puede haber grandes empresas que doten de capacidad computacional a X número de mineros, incentivando el potencial beneficio de forma individual, desincentivando la competencia y por tanto desincentivando el prestigio de la red. A día de hoy se sabe que el 50% del poder minero de la red Bitcoin es controlada por 8 grupos de mineros distintos, y para la red de Ethereum se cuantifican en 5. Se desconoce si son habilitadas por una o varias organizaciones, ni si estas son públicas o privadas. El anonimato de la red blockchain lo hace imposible. (Xiao, 2020).

La tolerancia de errores en el proceso de consenso de las redes públicas, las condiciones que de esta tipología se derivan y las limitaciones que dichas condiciones provocan, impiden una globalización de la tecnología. Al mismo tiempo, las empresas se han desarrollado para encontrar su nicho de mercado y no quedarse atrás con la irrupción de la Blockhain. De este modo estas adaptan su modelo de negocio a una tecnología Blockhain en la que solo sus afiliados o clientes pueden hacer uso de la misma, fomentando así la introducción de las redes blockchain *permissioned*. Una red *permissioned* es aquella que solo puedes ser partícipe si hay permiso expreso de algún nodo competente. Se requiere revelar la identidad de cada uno de los participantes y la dirección y consenso de la red es competencia de un grupo de individuos autorizado o por una empresa externa. Con la necesidad de revelar la identidad la red, en comparación con la pública, la hace ideal para realizar operaciones dentro de una misma empresa. El proceso de consenso para añadir bloques a la cadena resulta mucho más eficiente, capacitándola para procesar grandes cantidades de TPS. (Xiao, 2020). Es el caso de el Banco Santander, el cual utiliza la red de autorización *Ripple* o *permissioned* para hacer efectivas

transacciones entre sus clientes y así hacerse hueco ante las nuevas tendencias tecnológicas. (FinTech.es).

## 1. Comparación y el trilema de Seguridad-Descentralización-Escalabilidad

En el desarrollo de las redes blockchain de la actualidad, el sistema de consenso a aplicar en las plataformas ha ido acompañado de un proceso basado en la prueba y el error. Nakamoto, anticipándose a una crecida exponencial de usuarios en la red de Bitcoin, creó la regla del salto a la cadena más larga para evitar la propagación de las ya conocidas *forks* y fijó un intervalo de tiempo para el registro de los mismos. Con la aparición de Ethereum se adopta un sistema para reducir ese intervalo y aumentar las TPS, aceptando la aparición de más cadenas de bloques *fork*, pero haciendo de esta su aparición una ventaja y no una desincentivación para los mineros. (Xiao, 2020). A lo anterior se le añade la problemática del gran consumo de energía que del protocolo de consenso y minado se deriva, a lo que Ethereum responde con un sistema alternativo que quiere implementar en su forma 2.0, el *PoS*, el cual reducirá drásticamente el consumo de energía para las transacciones y la creación de bloques sin que esto signifique un descenso de la seguridad. (Pilkington, 2016)

Las blockchain surgidas después de 2016 parecen estar experimentando nuevos procesos y combinaciones de consenso utilizando las teorías disponibles, la computación distribuida, la criptografía y la computación fiable más allá del PoW y el *PoS*. Estas se encuentran fuera del objetivo de este trabajo, por lo que el lector si es deseo del lector saber más tipologías de métodos de consenso puede referirse a la bibliografía. Si que, con la aparición de tantos protocolos de consenso, se hace necesario un diseño equitativo del mismo según los objetivos que tenga la red para con la seguridad, la descentralización y la escalabilidad. (Xiao, 2020).

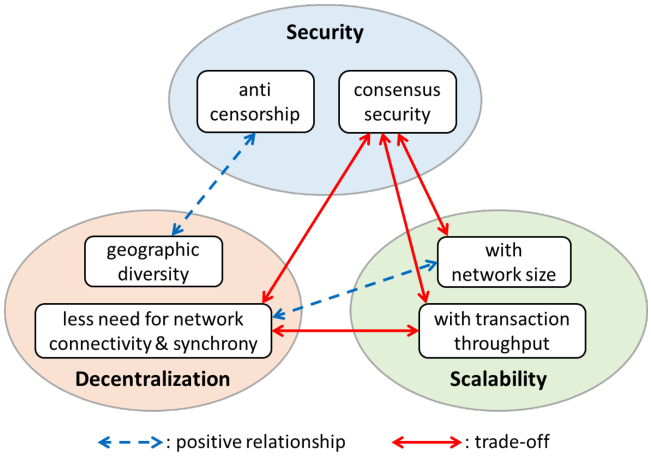



Figura 10: Ilustración del trilema de Seguridad, Descentralización y Escalabilidad.
Fuente: Xiao, 2020

**Seguridad:** Seguridad referida a la presencia de nodos perversos y el establecer un protocolo de consenso acorde a la no centralización de poder.

**Descentralización:** Defiende la idea del perfil descentralizado de una red blockchain, la globalidad, la diversidad, la conectividad y la sincronía entre participantes sin la presencia de partes mediadoras.

**Escalabilidad:** La capacidad de crecer de forma indefinida de una red, sin que esto se traduzca en un menor rendimiento de la misma. (Xiao, 2020).

Entonces, la afirmación siguiente, el comportamiento o la evolución de una red blockchain por lo que a número de transacciones representa será distinto según el protocolo de consenso que condicione la red, cobra sentido. Las redes de autorización o *permissioned*, en su mayoría, usan el protocolo de consenso llamado *BFT-style* que permite realizar miles de TPS en una red, dado su proceso de validación y consenso centralizado mucho más eficiente que, por ejemplo, el PoW de las redes públicas. Son generalmente pequeñas de unos miles de usuarios, pero altamente escalables. (Xiao, 2020). Es idóneo para empresas que deseen tener su red blockchain privada (p. ej. El Banco Santander o IBM). (Pilkington, 2016). Por lo que respecta las grandes redes, generalmente públicas estas, el protocolo de consenso sigue una relación probabilística, acuérdese del supuesto del 51% de los mineros honestos para el PoW en el que se asume este es honesto. La probabilidad se deriva de las posibilidades reales de que este no lo sea. Esto se traduce en gran presencia de usuarios, pero en solo unas pocas TPS.

Si relacionamos la afirmación anterior con la necesidad de definir un protocolo de consenso que se adapte a los servicios de la red, desembocamos en el conocido como trilema de Seguridad-Descentralización-Escalabilidad en el que se encuentran las blockchain públicas a día de hoy. Para muchas de las redes blockchain, la seguridad es una de las prioridades. Si bien es cierto que el nivel de seguridad puede ser objeto de cambio para obtener un sistema escalable. Menor nivel de seguridad, se traduce en mayores niveles de escalabilidad. El ejemplo más claro son las redes *permissioned* o, lo que es lo mismo, las grandes corporaciones en la actualidad. Para los protocolos *BFT*, su estructura de red pequeña se traduce en eficiencias para con la seguridad. Para muchas blockchain públicas que usan el protocolo de consenso de Nakamoto la alternativa descentralizadora y la seguridad como pilar fundamental para generar esa confianza entre usuarios que le caracteriza, impide que sea escalable a escala global. Por lo que a descentralización y probabilidad de ataques de nodos malignos respecta, las redes públicas usan los incentivos o limitan alguna fase de las transacciones para desincentivar la mala praxis dentro de la misma. Por último, pero no por ello menos importante, un diseño de protocolo ha de tener en cuenta que la repercusión de uno descentralizado y escalable, implica limitaciones

graves de seguridad. El protocolo de consenso de Nakamoto se basa en una potencia minera muy fuertes, contra mayor sea esta, mejor, pero siempre manteniendo un tiempo de generación de bloques para así desincentivar la aparición del *double spending issue*. Por otro lado, las redes basadas en el sistema *BFT* cada participante opera revelando su identidad, y dado que la red es pequeña y esta adherida a sistemas centralizados con poder permite gran número de TPS. Si bien lo anterior es cierto, cabe destacar que los sistemas de autorización o *permissioned* encuentran limitaciones de costes dada la constante y necesaria sincronización y conectividad entre miembros de la red, algo que no la hace escalable. (Xiao, 2020) (Zheng Z. X., 2017) (Zheng Z. X., 2018) (Swanson, 2015)

# VII. ¿CUÁL ES EL SIGUIENTE PASO?

Es esperanzador pensar en todo lo que la tecnología blockchain puede aportar a la sociedad, y siguiendo lo que se apuntaba al principio del trabajo sobre las expectativas, se quiere arrojar luz en la trayectoria que esta seguirá. El lector, con lo visto anteriormente, sabe que el objetivo final de la tecnología blockchain es dar una vuelta de hoja al sistema económico tradicional, y quiere hacerlo de la mano de la web e internet.

La web, a día de hoy asentada en la sociedad, también está en constante cambio, un cambio que empezó con la invención del ordenador personal, que le siguió la irrupción del *world wide web* con la llegada de Internet y se hizo global con las plataformas online centralizadas. Hablamos de Facebook, Airbnb, Google, Skype, Twitter, YouTube o Uber, entre muchas otras. El potencial que estas ofrecieron a la sociedad fue tal, que cambió el rumbo económico creando un escenario lleno de posibilidades. blockchain también persigue ser global, pero para ello son precisos dos factores muy importantes, por un lado, las facilidades de conectividad entre individuos y entre dispositivos que ofrecerá el IoT y un sistema de plataforma descentralizado totalmente escalable. (Zheng Z. X., 2018)

El alcance de la tecnología, en lo que se supone será el medio plazo, es muy diverso, y en conjunción de lo que se ha expuesto hasta el momento se estipula lo siguiente. El uso de redes *permissioned* como *Ripple,* hechas para y por entidades centralizadas seguirá creciendo, y lo hará de la misma forma que la necesidad irá aumentando con el cambio. Para lo que respecta al modelo globalizador que persiguen las redes públicas, una de las aplicaciones más esperadas al medio plazo es la de dar acceso a servicios bancarios y financieros a colectivos que hasta día de hoy, por su condición económica u cualquier otro impedimento, no disfrutaban de uno.

En un mundo globalizado se consumen todo tipo de bienes, pero su proceso de distribución resulta poco transparente para el consumidor final. Con una red blockchain detrás de una cadena de suministros se consigue un registro compartido, inmutable y sobretodo rastreable para saber el origen y las transformaciones experimentadas en ella. Se podrá hacer un seguimiento de la posesión de un bien a lo largo de todo su recorrido. Del mismo modo se podrá comprobar las condiciones de almacenamiento de los productos en barcos, camiones o aviones, así como la temperatura o la ubicación en tiempo real, garantizando que un producto se manipuló de forma segura y cumpliendo con las normas de seguridad y salubridad. Con el proyecto de IBM, grandes compañías del sector de la distribución como Carrefour ha reportado que se traduce en un beneficio directo para el cliente final. (Pilkington, 2016) (Xiao, 2020)

# VIII. CONCLUSIONES

La tecnología blockchain ha demostrado el potencial que tiene para dar un vuelco al sistema industrial tradicional, atendiendo sus características fundamentales: la descentralización, el anonimato de los usuarios, la veracidad de los datos de su registro y la persistencia de los mismos para formar la cadena. En este trabajo se ha tratado la tecnología blockchain como un activo revolucionario que presenta un paradigma totalmente nuevo para una economía y una reforma de un sistema social que le cuesta adaptarse al ritmo de vida de los individuos a los que ha de referirse. Buena prueba de ello es la puesta en evidencia de uno de los pilares de cualquier sistema capitalista, los bancos y las entidades financieras, siendo estas las primeras que verán, si no ya, el efecto disruptivo de la tecnología blockchain.

Los cambios al principio pueden percibirse amenazantes, pero con el tiempo se convertirán en una oportunidad de crecer para todo aquel que se haya adaptado, eclipsando a los que lo hayan desestimado. Un proceso de adaptación que muchas corporaciones están llevando a cabo de forma privada, adoptando su sistema centralizado a la tecnología blockchain. Las redes *permissioned* son ideales para el crecimiento empresarial y no ven más allá del beneficio corporativo, mientras que la Blockhain *permissionless* quiere llegar a ser el elemento clave para crear, junto al IoT y el análisis a gran escala o *Big Data,* el siguiente estadio de las conexiones definido como la *Web 3.0*, para crear así el *Global Cloud Computer (GCC).*

Un *GCC* de redes Blockhain y la suposición de realidad del IoT, se presume este rediseñaría el modelo web, hoy basado en la centralización debido a la desconfianza que la misma provoca por si sola, hacia una red global donde cada individuo pueda participar de la manutención del valor y propiedad registrado en la cadena. La Web 3.0 permite plantear un ecosistema totalmente independiente de organizaciones centralizadas y lleno de nuevas relaciones Peer-to-peer gracias a nuevos protocolos de internet. Por ejemplo, cada uno puede establecer su red de interacción entre individuos. En estas redes se prevé el individuo podrá intercambiar cualquier tipo de valor, ya sea este una moneda, propiedades, energía, el uso de una plaza de aparcamiento o el número de seguidores que uno tiene en las redes, como si estos fueran tokens. Los tokens como incentivo y vinculo entre usuarios, son genéricos y totalmente fungibles. El sistema monetario tradicional no es del todo fungible dado que hay ciertos aspectos a los que no les da valor directo, como por ejemplo un *like* en las redes sociales no es cuantificable monetariamente hablando. Los tokens reciben la característica de genéricos por el hecho de que dan utilidad y por tanto valor al cambio, ya sea este, cultura, sociedad o naturaleza. Por ejemplo, uno sabe cuanto cuesta una prenda de ropa por su calidad, la reputación de marca, la oferta y la demanda de la misma, entre otras, pero al precio no se le repercute cuánto ha contaminado la industria textil o incluso las condiciones en las que han trabajado sus empleados para producirla, por el

simple hecho de que la sociedad, aunque le de importancia, no puede cuantificar su utilidad en un contexto económico industrial, pero con la revolución tecnológica blockchain sí será posible.

De este modo el objetivo a largo plazo de la red blockchain es proporcionar un espacio seguro, confiable y programable de forma globalizada, donde gracias a las posibilidades del Web 3.0, una comunidad formada por todo el planeta pueda dar utilidad a aspectos intangibles a día de hoy incuantificables, pero de vital importancia. Son ejemplos la cultura, la contaminación, las condiciones laborales, el reciclaje, el uso de red wifi, entre muchas otras. Esto constituiría lo que se conoce como *Token Economy,* todo un reto para la sociedad en su conjunto más amplio.

## AGRADECIMIENTOS

El trabajo descrito ha sido respaldado por la institución Universitat de Barcelona. Al autor le gustaría agradecer al Dr. Eudald Puig, tutor del proyecto, su disposición y contribución con comentarios constructivos en todo momento.

# IX. BIBLIOGRAFÍA

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform.* White paper.

Frantz, C. K. (2016). *From institutions to code: Towards automated generation of smart contracts.* IEEE.

IBM. (2019). *IBM Annual Report 2018.*

Kehrli, J. (22 de Noviembre de 2016). *Niceideas.* Obtenido de https://www. niceideas. ch/roller2/badtrash/entry/blockchain-2-0-frombitcoin

Mattila, J. (2016). *The Blockchain Phenomenon.* Berkeley Roundtable of the International Economy.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Manubot.

Navarro, B. Y. (2017). *Blockchain y sus Aplicaciones.* Universidad Católica Nuestra Señora de La Asunción.

Nofer, M. G. (2017). *Blockchain.* Springer.

Pilkington, M. (2016). *Blockchain Technology: Principles and Applications.* Edward Elgar Publishing.

Saunders, A., & Cornett, M. M. (2019). *Financial Markets and Institutions.* New York: Mc Graw Hill Education.

Solomon, M. (20 de Abril de 2018). *Medium.* Obtenido de Using APIs in Your Ethereum Smart Contract with Oraclize: https://medium.com/coinmonks/using-apis-in-your-ethereum-smart-contract-with-oraclize-95656434292e

Swanson, T. (2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.* Report, avaliable online.

Szabo, N. (1997). *Formalizing and securing relationships on public networks.*

Tapscott, D. &. (2016). The Impact of the Blockchain Goes Beyond Financial Services. *Harvard Business Review*, 2-5.

Xiao, Y. Z. (2020). *A survey of distributed consensus protocols for blockchain networks.* IEEE Communications Surveys & Tutorials.

Zheng, Z. X. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends.* In 2017 IEEE international congress on big data (BigData congress): IEEE.

Zheng, Z. X. (2018). *Blockchain challenges and opportunities: A survey.* International Journal of Web and Grid Services.

# X. WEBGRAFÍA

https://www.blockchain.com/charts

https://etherchain.org/charts/transactionsPerDay

https://www.fin-tech.es/2016/05/santander-lanza-una-aplicacion-de-pagos-basada-en-blockchain.html

https://digiconomist.net/bitcoin-energy-consumption

https://digiconomist.net/ethereum-energy-consumption

https://medium.com/coinmonks/using-apis-in-your-ethereum-smart-contract-with-oraclize-95656434292e

# XI. ANEXO

## Anexo 1

Funcionamiento básico de la *state transition function*

*APPLY (S, TX) -> S' or ERROR*

Siendo:

S = Saldo inicial o state

TX = Transacción en curso

S' = Posición final o *State'*

El proceso para validad y procesar una transacción se puede resumir como se presenta a continuación:

1. *For each input in TX:*
   - *If the referenced UTXO is not in S, return an error.*
   - *If the provided signature does not match the owner of the UTXO, return an error.*
2. *If the sum of the denominations of all input UTXO is less than the sum of the denominations of all output UTXO, return an error.*
3. *Return S' with all input UTXO removed and all output UTXO added.*

Ejemplo adaptado al Sistema bancario tradicional

*APPLY ({ Alice: $50, Bob: $50 },"send $20 from Alice to Bob") = { Alice: $30, Bob: $70 }*

Pero:

*APPLY ({ Alice: $50, Bob: $50 },"send $70 from Alice to Bob") = ERROR*

**Anexo 2**

*DURATION GAP MODEL*

La duración se define como la media ponderada de tiempo hasta madurez de una inversión teniendo en cuenta el valor actual de los *cash flows* ponderados.

Se asume duración como indicador económico de sensibilidad o elasticidad ante cambios de tipo de interés de mercado dado un activo y pasivo indexados a tales medidores.

Típicamente usado para calcular el riesgo de exposición de instituciones financieras, dada su naturaleza mercantil, se entiende como una medida de impacto real para cualquier otra empresa que disponga o dependa de activos o pasivos, respectivamente indexados a un tipo de interés variable y a una madurez dispar.

Para estimar la diferencia de duración de una empresa, se ha de determinar la duración de sus activos y de sus pasivos. La duración de un portafolio de activos y pasivos será el peso ponderado del precio de mercado de dichos componentes. Para el ejemplo se considera un único componente para cada partida del balance.

Del balance se deduce lo que sigue:

$$A = P + PN$$

y:

$$\Delta A = \Delta P + \Delta PN$$

o:

$$\Delta PN = \Delta A - \Delta P$$

Cuando hay un cambio en el tipo de interés, el patrimonio neto de la empresa resulta en la diferencia de cambios en el activo y el pasivo.
Como ΔPN= ΔA- ΔP, se ha de determinar como los cambios de valor en los activos y pasivos del balance se relacionan con su duración:

$$\frac{\Delta A}{A} = -D_A \frac{\Delta R}{(1+R)}$$

y:

$$\frac{\Delta P}{P} = -D_P \frac{\Delta R}{(1+R)}$$

El termino ΔR/((1+R)) no es más que el *shock* del cambio porcentual de tipo de interés. La ecuación se podría expresar de la siguiente manera:

$$\Delta A = A\,(-D_A)\frac{\Delta R}{(1+R)}$$

y:

$$\Delta P = P(-D_P)\frac{\Delta R}{(1+R)}$$

Siendo ΔPN= ΔA- ΔP, se puede sustituir en la expresión anterior. Con dicha combinación, la ecuación resulta en una medida de cambio de estado del patrimonio de una empresa:

$$\Delta PN = -(D_A - kD_P)\,A\,\frac{\Delta R}{(1+R)}$$

Donde:

k = P/A; Mide el apalancamiento de la empresa. La cantidad de recursos ajenos que financian los activos de los propietarios.

La afectación de un cambio en el tipo de interés de mercado, devalúan el patrimonio de la empresa (ΔPN) en los siguientes supuestos:

1. Apalancamiento ajustado a la duración = $D_A - kD_P$. En años y refleja el desequilibrio de duración en el balance de una empresa. En esencia, cuánto mayor sea el desequilibrio, mayor exposición al riesgo de tipo de interés.
2. El tamaño de la empresa. Cuánto mayor sea el activo de la empresa, mayor es el riesgo de tipo de interés de sus activos, y por tanto de su valor, ante cualquier *shock.*
3. El tamaño del *shock* de tipo de interés = ΔR/((1+R)). Cuánto mayor sea el impacto, mayor será la exposición de la empresa. Atendiendo una afectación igual tanto en sus activos como en los pasivos.