

Protocols d'Internet - Trabajo escrito

Blockchain

Albert Bernal y Adrián Rubio

18/06/2021

ÍNDICE

1. Introducción	2
2. Historia	3
2.1 Primeros pasos	3
2.2 Bitcoin y sus consecuencias	4
2.3 El papel de blockchain en la actualidad	4
3. Definición	6
3.1 Tipos	7
4. Funcionamiento	7
4.1 Algoritmo de consenso	8
5. Aplicaciones	9
6. Conclusiones	11
7. Referencias	12

1. Introducción

Debido al pleno auge en el que está actualmente el tema de las criptomonedas, no es raro ver cómo se opina y habla de la tecnología *blockchain*, en numerosas ocasiones usándola como una palabra que está de moda, sin saber realmente qué implica y cuáles son sus virtudes y defectos. Principalmente, esta es la razón que nos impulsó a escoger este tema para hacer el trabajo escrito. Además, *blockchain* es un tema que, visto desde fuera, nos parece interesante debido a que se trata de un mercado en constante crecimiento y que, incluso, podría resultar útil personalmente a nivel laboral, ya que, por ejemplo, tiene usos en ámbitos tan relevantes para nuestra rama del grado como el IoT. Entre nuestros objetivos se encuentran conocer esta tecnología, mostrar que no sólo es Bitcoin y entender su potencial. Para ello, evitaremos adentrarnos demasiado en aspectos técnicos, pese a que los comentaremos de forma general.

Creemos que una buena estructura para el trabajo es la siguiente: para empezar, haremos un recorrido por sus inicios, desde el motivo de su invención hasta la expansión mundial que ha sufrido y parece que seguirá sufriendo en los próximos años. Más adelante, veremos en qué consiste realmente una cadena de bloques y cómo es posible que sea tan segura y que a la vez, se administre automáticamente. Por último, teniendo en cuenta su funcionamiento, analizaremos las distintas aplicaciones en las que nos podemos beneficiar del uso de *blockchain* y conseguir así, una visión de futuro para una tecnología a la que aún le queda mucho por recorrer.

How to Time-Stamp a Digital Document

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Figura 1. Inicio del documento original de la primera publicación sobre *blockchain*

2. Historia

Pese a que el reciente auge en la popularidad de la tecnología de *blockchain* de la mano de las criptomonedas podría llevar a entender que se trata de una tecnología con pocos años de vida, la idea detrás de ella se remonta a principios de los 90, mientras que la primera implementación, que encontramos en el mantenimiento de registros para la criptomoneda Bitcoin, data del 31 de octubre de 2008.

2.1 Primeros pasos

La idea detrás de la tecnología *blockchain* fue descrita por primera vez en 1991 por Stuart Haber y W. Scott Stornetta cuando introdujeron una solución computacionalmente práctica para sellar documentos digitales con un *timestamp* para que no pudieran tener una fecha anterior o ser alterados.

Se trataba de un sistema de jerarquía digital llamado “cadena de bloques”, y fue presentado en un estudio en la revista *Journal of Cryptology* en 1991 llamado *How to time-stamp a digital document*. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004, cuatro años antes de los inicios de Bitcoin. Pese a no obtener ningún tipo de repercusión por casi dos décadas, el estudio de estos dos científicos sentaría las bases para la revolución de la tecnología *blockchain* del siglo XXI, mucho antes de que Satoshi Nakamoto, el pseudónimo usado por la persona o grupo de personas que crearon Bitcoin, presentará dicha tecnología en 2009.



Figura 2. Stuart Haber, izquierda y Scott Stornetta, derecha, en 1990

Un año después de su primera publicación, en 1992, los mismos autores presentaron un nuevo estudio con mejoras llamado *Improving the Efficiency and Reliability of Digital Time-Stamping*. Se incorporaron árboles de Merkle al diseño, haciéndolo más eficiente al permitir que varios documentos fuesen recopilados en un mismo bloque.

En 2004, Hal Finney, un científico informático, introdujo un sistema llamado RPoW, *Reusable Proof Of Work*. Éste podría ser considerado como un prototipo y un paso significativo en la historia de las

criptomonedas, ya que resolvió el problema del doble gasto¹ al mantener la propiedad de los tokens registrada en un *trusted server* que fue diseñado para permitir a los usuarios de todo el mundo verificar su exactitud e integridad en tiempo real. El sistema funcionaba recibiendo un token no intercambiable y enviando uno firmado por RSA que podía ser transferido entre personas.

2.2 Bitcoin y sus consecuencias

A finales de 2008 fue publicado un artículo bajo el nombre de Satoshi Nakamoto con el título *Bitcoin: A Peer-to-Peer Electronic Cash System*. Entraremos en más detalle en el apartado de funcionamiento pero, en pocas palabras, consistía en una idea muy parecida a las descritas anteriormente, con la diferencia de que la protección ante el doble gasto (y consecuentemente la fiabilidad de las transacciones) era proporcionada por un protocolo *peer-to-peer* descentralizado: un bitcoin era minado por un usuario particular usando *proof-of-work* y después era verificado por los nodos descentralizados de la red, es decir, los demás usuarios. Por lo tanto, eso suponía que para que se valide una transacción, los demás la deben aceptar como correcta.

Como curiosidad, el primer bloque fue minado el 3 de enero de 2009 por Satoshi Nakamoto y obtuvo 50 bitcoins como recompensa y la primera transacción fue realizada el 12 de ese mismo mes, cuando Satoshi envió 10 bitcoins a Hal Finney, el científico autor de RPoW.

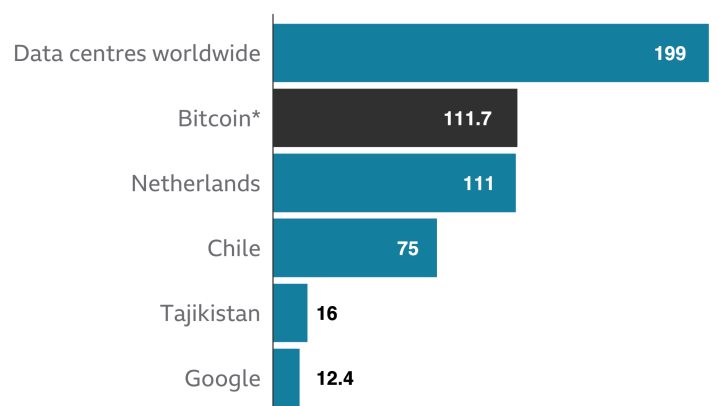
Bitcoin representó para *blockchain* un escaparate, una muestra de su utilidad. No obstante, durante los primeros años, el crecimiento en la popularidad de ambas fue casi negligible. Fue a partir del 2013 cuando algunas empresas empezaron a fijarse en la tecnología con otros objetivos en mente, con usos más allá de mantener el registro de criptomonedas. Esta nueva forma de entender las transacciones entre dos entidades, que evita la necesidad de un intermediario, podría tener un claro impacto en la eficiencia de cadenas de suministro, transporte, seguridad social o seguros, entre otros. En los siguientes años su uso no ha hecho más que crecer, sobre todo en sectores como la banca y las aseguradoras.

2.3 El papel de blockchain en la actualidad

En los últimos años, coincidiendo con el gran *boom* de las criptomonedas, la adopción de tecnologías como *blockchain* y sucedáneas está sufriendo un crecimiento importante, aunque a menor escala. Pese a que el aumento de su popularidad es un factor relevante, lo es más el hecho de que se estén destinando cantidades ingentes de dinero a su investigación, con la intención de introducir mejoras y dejar atrás el

¹ El doble gasto es un potencial problema de las criptomonedas que consiste en poder usar las mismas unidades para dos transacciones distintas mediante la reproducción de monedas falsificadas.

proof-of-work para sustituirlo por conceptos más eficientes, sobre todo a nivel de la obtención de bloques. No hay que olvidar el papel destructor que tiene el minado sobre el medio ambiente, siendo un proceso de alto consumo de energía.



*All figures 2019 except Bitcoin, which is annualised middle estimate for bitcoin electricity consumption in January 2021

Source: Forbes, IEA, EIA, Cambridge Centre for Alternative Finance

BBC

Figura 3. Consumo anual de energía, en TWh

Como podemos observar en la figura, el consumo anual de la obtención de bitcoins es comparable al de un país del primer mundo como los Países Bajos, de más de 17 millones de habitantes. Es un claro problema que se espera solucionar con nuevas soluciones de autenticación menos costosas.

La transición relevante con más posibilidades de llevarse a cabo a día de hoy es la de pasar de *proof-of-work* a *proof-of-stake*. Esta nueva manera de comprobar que las transacciones son legítimas es más eficiente y por lo tanto más respetuosa con el medio ambiente. No tiene bloques y la recompensa para el que realiza el cálculo del algoritmo para comprobar la legitimidad es una tarifa aplicada sobre la transacción. Entre los impulsores de este cambio encontramos, entre muchos otros, los desarrolladores de la segunda criptomoneda con más valor del mercado, Ethereum.

Antes de finalizar este apartado, creemos necesario mencionar dos posturas por parte de gobiernos estatales, empezando por el de China. El suyo es un caso muy particular porque cuenta con un enorme capital humano, crucial en el desarrollo de futuras mejoras para *blockchain*, pero tiene un gobierno que está completamente en contra de las criptomonedas, tanto que las han prohibido². Pese a ello, la investigación en las tecnologías como Neo, la primera plataforma *blockchain* descentralizada de código abierto fundada en China, puede seguir su curso. Es incluso apoyada por empresas de la talla de Alibaba, un gigante del comercio electrónico que, como la gran mayoría de compañías chinas de esa

² China's Crypto Crackdown Intensifies With New Mining Ban And Censorship—But Bitcoin Is Rallying <https://www.forbes.com/sites/jonathanponciano/2021/06/09/chinas-crypto-crackdown-intensifies-with-new-mining-ban-and-censorship-but-bitcoin-is-rallying>

magnitud, tiene el apoyo del gobierno. Esta paradoja difumina la imagen que da el gigante asiático sobre su postura, y hace difícil predecir si habrá cambios de opinión en un futuro.

El segundo caso es el de El Salvador, relevante desde hace muy poco tiempo, alrededor de una semana antes del redactado de este apartado. La suya es una postura completamente opuesta, ya que el día 9 de junio se aprobó una ley³ que obliga a "todo agente económico a aceptar bitcoin como forma de pago". Las consecuencias de esto son que se permite que se paguen los impuestos con bitcoin y establece que todas las obligaciones en dinero expresadas en dólares previas a la emisión de la ley podrán ser pagadas en bitcoin. Es un cambio impulsado por el joven presidente del país Nayib Bukele, un jefe del estado poco convencional que ha alterado la política del país y es uno de los principales defensores de las criptomonedas a nivel mundial. El 17 de junio, el Banco Mundial emitió un comunicado en el que dijo que no apoyará al gobierno salvadoreño con su proyecto.

En conclusión, *blockchain* es y aparentemente será una tecnología en constante evolución, que ha pasado del desconocimiento a tener un papel muy importante en la sociedad actual y cuyo progreso los próximos años será, sin lugar a dudas, muy interesante.

3. Definición

Blockchain como su nombre indica, es una cadena de bloques. Esta cadena en definitiva, es una base de datos que, en lugar de almacenar la información en tablas como en la mayoría de casos, la almacena en bloques que se relacionan entre sí. Pese a que existen distintos tipos que explicaremos seguidamente, en esta definición nos centraremos en la *blockchain* pública. Lo que hace tan especial a esta tecnología es el hecho de que los datos, en vez de estar regidos y controlados por un organismo o conjunto de organismos central (como podría ser una empresa, un banco o un gobierno) se regulan de manera autónoma, sin depender de un administrador que verifique la validez de los datos almacenados y que proteja la integridad de éstos. Esto *blockchain* lo consigue gracias a que la información se almacena en bloques y cada bloque está relacionado con el anterior de la cadena, la información de la cadena se guarda en varios nodos que replican esta información, así si todos los nodos contienen la misma cadena se puede verificar la veracidad de los datos, si no fuera así se detectaría un ataque o un error en el sistema. Con esto se consigue que la información almacenada en los bloques sea perpetua e inmutable, en el siguiente apartado explicaremos con más detalle su funcionamiento.

³ Bitcoin: El Salvador makes cryptocurrency legal tender, BBC, 2021
<https://www.bbc.com/news/world-latin-america-57398274>

3.1 Tipos

La categorización más común la divide en cuatro grupos:

- **Pública:** Este es el tipo más conocido, sobre todo por ser el que usan las criptomonedas como Bitcoin. Se trata de un modelo descentralizado con la información distribuida (DLT, *Distributed Ledger Technology*). Sus ventajas son la independencia de organizaciones, la transparencia y la fiabilidad en cuanto a la integridad de los datos. Sus inconvenientes son principalmente el rendimiento y la escalabilidad. Se usa en criptomonedas y validación de documentos.
- **Privada:** En este caso la *blockchain* funciona en un ambiente restringido, como una red privada, y está controlada por una única entidad. Sigue teniendo el mismo funcionamiento, con conexiones *peer-to-peer* y descentralización, pero no puede ser usada por alguien no autorizado por la empresa. Sus ventajas son el poder controlar el acceso de los usuarios y el rendimiento, superior ya que se trata de una menor escala. Sus inconvenientes son la fiabilidad, transparencia y auditabilidad. Se usa en cadenas de suministro y gestión de la propiedad de bienes.
- **Híbrida:** Consiste en combinar las dos anteriores, teniendo control sobre qué partes son públicas y cuáles privadas mediante un sistema de permisos. Sus ventajas e inconvenientes son los de los apartados anteriores para cada una. Se usa en el mantenimiento de registros médicos y en gestión de inmuebles.
- **Consortio:** Se trata de una *blockchain* privada pero que en esta ocasión es gestionada por más de una entidad. Tiene las mismas ventajas e inconvenientes que las privadas pero con una mayor fiabilidad debido a tener más de una organización propietaria. Se usa mayoritariamente en la banca y también en cadenas de suministro.

4. Funcionamiento

Antes de empezar con el funcionamiento en sí de la tecnología *blockchain* debemos entender qué tipo de red utiliza, se trata de una red *Peer-to-Peer*. Este tipo de red se basa en un conjunto de nodos que se comportan como iguales entre sí, es decir, una red descentralizada donde mediante un protocolo de comunicación común, los nodos se envían y reciben todo tipo de información directamente sin necesidad de intermediarios.

Como ya hemos mencionado en la definición, todo gira en torno a una cadena de bloques (registros) que almacenan información sobre (por ejemplo) transacciones de una cuenta bancaria y un conjunto de nodos que almacenan copias de ésta. Los registros contienen el identificador (hash) del bloque anterior en la cadena además de la información que contiene dicho bloque. A partir de este contenido se aplica

una función de hash⁴ para darle identificador al bloque “nuevo”. De esta manera se consigue que cada bloque de la cadena, excepto el primero, dependa del anterior, de modo que si se modifica alguno de los bloques de la cadena, ésta se rompe, ya que entonces el hash del bloque modificado cambiaría y se rompería el enlace con el siguiente. Entonces si en una *blockchain* quisiéramos modificar algún registro, deberíamos modificar todos los que le suceden, y re-calcular el correspondiente hash para cada uno, este proceso normalmente comporta un alto coste computacional que aumenta exponencialmente en función del número de bloques. Cada vez que se quiera añadir un nuevo bloque, se deberá buscar un hash que cumpla con los requisitos ya establecidos. Este proceso se denomina minado y lo realizan un subgrupo de los nodos que componen la red. Además, para escoger quién puede añadir un nuevo bloque a la cadena existen los algoritmos de consenso, de lo que hablaremos a continuación. Una vez se consigue un nuevo bloque para la cadena, se actualiza la información del resto de nodos de manera simultánea.

4.1 Algoritmo de consenso

Uno de los aspectos más importantes de la red *blockchain* es determinar quién tiene la capacidad de agregar nuevos bloques a la cadena. Para ello, se utiliza un mecanismo de consenso distribuido. Si estamos en una red pública, el modelo de consenso utilizado premiará a los nodos que agreguen nuevos bloques a la cadena con bienes digitales (como las criptomonedas), por lo que habrá competencia entre diferentes nodos candidatos que sean capaces de publicar dichos bloques. El algoritmo arbitrará la creación de dichos bloques, determinará la dificultad de generar nuevos bloques, protegerá la red de usuarios malintencionados y permitirá que diferentes nodos generen bloques trabajando conjuntamente sin necesitar un alto nivel de confianza entre ellos. En una red privada, cuando encontramos que la confianza entre los nodos es alta, no es necesario proporcionar incentivos para los nodos mineros ya que, a mayor grado de confianza, menor coste computacional.

A continuación definiremos los dos principales algoritmos de consenso utilizados actualmente.

- **Proof Of Work (PoW):** este algoritmo de consenso es el más conocido por ser el modelo seguido por las principales criptomonedas como *Ethereum* o *Bitcoin*. Este tipo de algoritmo se basa en exigir a los nodos mineros computar problemas de coste muy elevado para conseguir añadir un nuevo bloque, estos problemas deben ser difíciles de computar pero una vez obtenida la clave tiene que ser fácil verificar su validez, para que, cuando un nodo encuentre

⁴ Algoritmo matemático de sentido único que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

Su utilidad reside en ser una familia de funciones $h : \{0,1\}^* \rightarrow \{0,1\}^l$ que:

1. Cuenta con funciones fáciles de calcular.
2. No es computacionalmente factible, dada una función h , encontrar un par de *strings* distintos x, x' que satisfagan $h(x) = h(x')$, hecho conocido como una colisión.

una posible solución los demás puedan verificar que es correcta de manera sencilla. Normalmente se exige que el hash obtenido tenga ciertas características para hacer así el cálculo más complejo. En el caso de Bitcoin, por ejemplo, aumentan la dificultad de cálculo exigiendo que el hash empiece con más o menos ceros, así para conseguirlo los nodos deberán ir modificando la cabecera introduciendo valores aleatorios (nonce) y generando hashes hasta conseguir la combinación que resulte un hash con los requisitos esperados. En el caso de que dos mineros añadan un bloque a la vez, se escogerá el que tenga la cadena más larga, es decir el que haya llevado más trabajo (Proof Of Work).

- **Proof of Stake (PoS):** como su nombre indica, en vez de regirse por la dificultad de obtención del nuevo bloque, este algoritmo se rige por la cantidad de participaciones que tenga el nodo. Entonces en este caso, la probabilidad de que un usuario añada un nuevo bloque es proporcional al número de tokens que este disponga. En base a esto se pueden aplicar distintas estrategias para discernir entre un usuario u otro como por ejemplo el tiempo que lleva el usuario en la red o la cantidad de transacciones que ha realizado.

5. Aplicaciones

Como hemos introducido en el apartado de historia, *blockchain* es una tecnología que se dio a conocer gracias a Bitcoin, pero cuyas utilidades han ido mucho más allá. Nuestra intención en este apartado es dar una idea general de la cantidad de ámbitos con casos de uso más que desarrollar con profundidad unos pocos ejemplos. Por ello, veremos un listado con explicaciones breves.

- **Sector financiero:** Dejando de lado la posible revolución de las criptomonedas, veamos algunos ejemplos de otros escenarios que se verían beneficiados por su utilización:
 - **Transacciones internacionales:** La globalización impulsa año tras año el crecimiento de este tipo de transacciones, que *blockchain* podría ayudar a ser más eficientes y seguras eliminando intermediarios. Por ejemplo, el banco Santander anunció en 2018⁵ un servicio de transferencias internacionales basado en *blockchain*.
 - **Gestión de inversiones:** Traería mejoras como facilitar la colaboración al permitir acceso fácil por todas las entidades a una única fuente de información; simplificar la validación de transacciones, ya que la transparencia de la cadena de bloques ayuda a cada parte a validarlas fácilmente; y mejorar la seguridad general de los datos, ya que, como hemos visto, éstos se almacenan en registros (teóricamente) inmutables.

⁵ Santander launches the first blockchain-based international money transfer service across four countries <https://www.santander.com/content/dam/santander-com/en/documentos/historico-notas-de-prensa/2018/04/NP-2018-04-12-Santander%20launches%20the%20first%20blockchain-based%20international%20money%20transfer%20service%20across%20-en.pdf>

- **Eliminación de burocracia:** El papel como tal está destinado prácticamente a desaparecer, pero la documentación en su formato digital no. La burocracia excesiva ralentiza cualquier proceso, y *blockchain* puede ayudar a minimizarla.
- **Reducir el error humano:** Este aspecto encaja en el apartado financiero como en cualquier otro, ya que está presente allí donde una persona forme parte de un proceso. *Blockchain* reduce esa posibilidad y ayuda a asegurar la integridad de los archivos.
- **Sector público:** Desgraciadamente, es muy común en cualquier sociedad el hecho de desconfiar del gobierno e instituciones públicas. Algunos ejemplos de aplicaciones son los siguientes:
 - **Voto electrónico:** Usar una tecnología basada en *blockchain* crearía un sistema mucho más robusto gracias a la descentralización del proceso de votación y ayudaría inmensamente en la transparencia de los resultados. El error humano, por ejemplo en el recuento, también se vería minimizado.
 - **Transparencia presupuestaria:** La historia reciente, por ejemplo en el caso de España, nos ha demostrado que no se puede confiar en todo el que hace uso de los fondos públicos. La fiabilidad y transparencia de *blockchain* ayudarían a reducir la corrupción.
- **IoT:** Pese a no ser tan relevante a día de hoy como los dos casos anteriores, lo será en un futuro próximo y está muy relacionado con la especialidad que cursamos. Primero veremos una breve justificación de su relevancia en unos años y a continuación explicaremos el papel de *blockchain*.

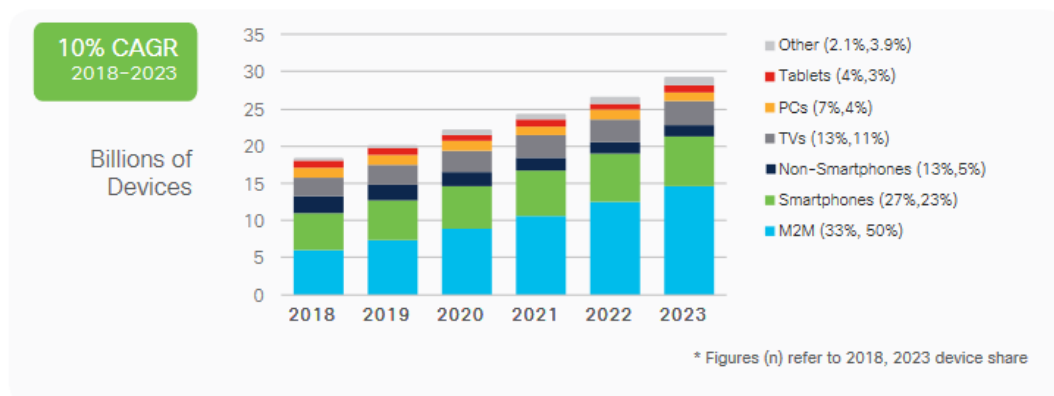


Figura 4. Cisco Annual Internet Report, Crecimiento global esperado de conexiones y dispositivos

La figura 4 es un claro ejemplo de que, a nivel mundial, los dispositivos y las conexiones crecen cada vez más rápidamente. Un número creciente de aplicaciones M2M (*Machine to Machine*), como videovigilancia, seguimiento de paquetes, transporte autónomo, contribuirán de manera importante al aumento de dispositivos y conexiones. Como se puede ver en la gráfica, Cisco prevé que, en 2023, las conexiones M2M representarán el 50% del total de dispositivos y conexiones, habiéndose multiplicado el número por un factor de 2.4 hasta los 14.700 millones de conexiones.

Este incremento influirá positivamente en el desarrollo de la *Internet of Things*, ya que se prevé que el 2023 cerca de la mitad de las conexiones M2M serán para aplicaciones de casas inteligentes, como automatización del hogar. Para el crecimiento de tráfico entre vehículos autónomos o para las *smart cities* tendremos que esperar más, pero su aumento también será notable.

En cuanto a los beneficios que puede aportar *blockchain* encontramos una mejora en la seguridad de los dispositivos, ya que aumentará la dificultad para cibercriminales de alterar datos como lecturas de sensores; un aumento en la transparencia de cara al usuario sobre qué datos recopilará la empresa; o simplemente aumentar la eficiencia del conjunto de dispositivos, ayudando a reducir el consumo de la red.

6. Conclusiones

Antes de empezar este trabajo, ya teníamos una imagen general de lo que era la *blockchain*, pero para nada teníamos idea del revolucionario cambio que ésta podía suponer. Primeramente, nunca hubiéramos pensado que una tecnología tan moderna tuviera sus inicios el siglo pasado, pero el caso es que la idea ya se puso en práctica hace tiempo, sólo que con el nacimiento y la popularización de Bitcoin este concepto de cadena de bloques empezó a salir a la luz. Lo que sí que sabíamos es que *blockchain* no era sólo Bitcoin, y esto ha quedado más que demostrado a lo largo del trabajo. Gracias a la investigación que hemos llevado a cabo durante la realización del trabajo, hemos descubierto su gran potencial y las múltiples situaciones en las que esta tecnología no solamente sería útil sino que también mejoraría en gran medida la seguridad y el gasto innecesario de tanto puestos de trabajo como material y tiempo. Tanta es la revolución que podría llegar a suponer un cambio cultural en el que no haga falta confiar en ninguna entidad para llevar a cabo ningún tipo de trámite, simplemente confiar en una futura versión de *blockchain* teóricamente imposible de vulnerar.

En conclusión, si bien es cierto que *blockchain* puede llegar muy lejos, esto no será posible sin la colaboración de entidades gubernamentales y empresas que deberán destinar parte de su inversión a la investigación de esta tecnología. El problema es que por ejemplo en el caso del Bitcoin ciertos países como China prohíben la moneda, y otros, en cambio, como El Salvador, la aceptan como moneda completamente válida para pagar impuestos o comprar todo tipo de bienes. Ésto da que pensar que a la evolución que esperamos aún le quedan varios años por delante dado que hay muchos intereses de por medio y no será un problema de rápida solución. Pese a ello, creemos que tendrá un progreso interesante para nosotros, el espectador, y estamos intrigados por ver qué pasará en los próximos años.

7. Referencias

Historia

A Brief History of Blockchain, Harvard Business Review, 2017

<https://hbr.org/2017/02/a-brief-history-of-blockchain>

How to Time-Stamp a Digital Document, Stuart Haber y W. Scott Stornetta, 1991

https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf

Improving the Efficiency and Reliability of Digital Time-Stamping, Stuart Haber y W. Scott Stornetta, 1992

https://www.researchgate.net/publication/2312902_Improving_the_Efficiency_and_Reliability_of_Digital_Time-Stamping

A Very Brief History Of Blockchain Technology Everyone Should Read, Bernard Marr, 2020

<https://bernardmarr.com/default.asp?contentID=1353>

Definición

Blockchain Definition: What You Need to Know, Investopedia, 2021

<https://www.investopedia.com/terms/b/blockchain.asp>

What is Blockchain Technology?, Blockgeeks, 2020

<https://blockgeeks.com/guides/what-is-blockchain-technology/>

Funcionamiento

PoW vs PoS, Blockgeeks, 2020

<https://blockgeeks.com/guides/es/prueba-de-trabajo-vs-prueba-de-participacion/>

Blockchain technology explained, Coding Tech, 2018

https://www.youtube.com/watch?v=qOvAbKKSH10&ab_channel=CodingTech

Aplicaciones

Blockchain Technology Applications & Use Cases in 2020, Business Insider, 2020

<https://www.businessinsider.com/blockchain-technology-applications-use-cases>

An Overview of Smart Contract and Use Cases in Blockchain Technology, Bhabendu Kumar Mohanta, Soumyashree S Panda, Debasish Jena, 2018

<https://ieeexplore.ieee.org/abstract/document/8494045>

Blockchain use cases, IBM, 2021

<https://www.ibm.com/blockchain/use-cases/>

What is IoT with blockchain, IBM, 2021

<https://www.ibm.com/topics/blockchain-iot>

Figuras

Figura 1: How to Time-Stamp a Digital Document, Stuart Haber y W. Scott Stornetta, 1991

https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf

Figura 2: The blockchain: Mythical Ends and Technical Means, Becker Friedman Institute, 2019

<https://bfi.uchicago.edu/wp-content/uploads/U-Chicago-2019.pdf>

Figura 3: How Bitcoin's vast energy use could burst its bubble, BBC, 2021




<https://www.bbc.com/news/science-environment-56215787>

Figura 4: Cisco Annual Internet Report (2018–2023) White Paper, Cisco, 2018

<https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>

Participación

1. Introducción	2
2. Historia	3
2.1 Primeros pasos	3
2.2 Bitcoin y sus consecuencias	4
2.3 El papel de blockchain en la actualidad	4
3. Definición	6
3.1 Tipos	7
4. Funcionamiento	7
4.1 Algoritmo de consenso	8
5. Aplicaciones	9
6. Conclusiones	11
7. Referencias	12

-  Albert Bernal
-  Adrián Rubio
-  Ambos