BLOCKCHAIN: UN TUTORIAL

*Carlos Zozaya, José Incera y Ana Lidia Franzoni**

RESUMEN: La innovadora tecnología con la que opera la criptomoneda *bitcoin*, llamada *blockchain*, permite el intercambio de valor entre individuos sin la necesidad de una autoridad central de confianza. En este artículo se da una explicación del funcionamiento general de *blockchain*.

BLOCKCHAIN: A TUTORIAL

ABSTRACT: The innovative technology behind the operation of the Bitcoin cryptocurrency, called the *blockchain* allows the exchange of value between peers without the need for a trusted central authority. In this paper, we provide an explanation of how the *blockchain* works.

PALABRAS CLAVE: bitcoin, firma digital, función hash, confianza.
KEY WORDS: bitcoin, digital signature, hash function, trust.

RECEPCIÓN: 27 de septiembre de 2017.
APROBACIÓN: 29 de enero de 2018.
DOI: 10.5347/01856383.0129.000294417

* José Incera y Ana Lidia Franzoni son integrantes de la División Académica de Ingeniería del ITAM; Carlos Zozaya forma parte de la empresa Técnica Administrativa BAL. Los autores agradecen a la Asociación Mexicana de Cultura, A.C. su apoyo en la realización de este trabajo.

BLOCKCHAIN: UN TUTORIAL

Introducción

La confianza en el mundo digital se pierde si no se mantienen la confidencialidad, integridad y reconocimiento de la información intercambiada. *Confidencialidad* implica que no se da a conocer información a individuos, entidades o procesos no autorizados; la *integridad* consiste en preservar la información completa y precisa durante todo su ciclo, de modo que los datos no pueden ser modificados subrepticiamente ni sin autorización. Por último, el *reconocimiento* es el acto del emisor de no negar que envió la información.

La estructura cadena de bloques, mejor conocida por su término técnico *blockchain,* tiene el potencial de transformar drásticamente el sector de los servicios financieros, así como otros aspectos de nuestra sociedad, dado que favorece la confianza en el mundo digital. Por eso, algunos expertos consideran que el *blockchain* es una de las tecnologías con más impacto desde la invención de internet,[1] y muchas compañías invierten miles de millones de dólares para desarrollar nuevos modelos de negocio en los que se aproveche la tecnología.

El término *blockchain* engloba varias interpretaciones. Algunas personas lo utilizan para designar la manera de registrar y almacenar las

[1] Don Tapscott y Alex Tapscott, *The blockchain revolution*, 2016, Nueva York, Penguin Random House.

transacciones de algunas criptomonedas, mientras que otras lo utilizan para describir otros componentes de un entorno de *blockchain*, incluyendo las reglas que determinan el comportamiento de dicho sistema. Los diferentes "sabores" que han surgido para indicar diversos componentes del *blockchain* han evolucionado rápidamente y no hay una norma universal para muchos de ellos. En este trabajo se utilizará el término *blockchain* de manera amplia. El objetivo es dar una panorámica general y no una comparación entre las distintas plataformas de esta tecnología.

Fundamentos técnicos

En esta sección se explica cómo funciona el ecosistema de *bitcoin*. Sin embargo, antes es necesario presentar dos conceptos técnicos que forman la base del *blockchain*: *1)* firmas digitales, que permiten al usuario validar y autentificar contenido digital, y *2)* funciones *hash* criptográficas, que permiten crear identificadores únicos para contenido digital. Ambos conceptos son fundamentales para dar seguridad e integridad en el sistema de *blockchain*.

Firmas digitales

Al igual que las firmas autógrafas, el objetivo de las firmas digitales es certificar el reconocimiento de una persona del contenido de un documento. En ambos casos, la firma está ligada al contenido del documento.[2]

Las firmas digitales cumplen con dos condiciones: *1)* solo una *persona*[3] puede "firmar" un documento con su propia firma, pero cualquiera que conozca la firma puede verificar que corresponde a esa persona en

[2] Esto es cierto para las firmas digitales, pero no necesariamente para documentos de varias páginas en los que la firma autógrafa se pone solo en la última página, pues podría ocurrir que se remplazara una página intermedia.

[3] En firmas digitales, el concepto de "persona" no necesariamente corresponde a un ser humano. Por ejemplo, una empresa o un alias pueden tener su propia firma.

particular; y *2)* la firma está ligada al contenido del documento firmado, de tal manera que es imposible "cortar y pegar" la firma en otro documento para validarlo.

Las firmas digitales se basan en algoritmos criptográficos asimétricos o de llave pública, en los que se utiliza un par relacionado de cadenas de bits (las llaves) para encriptar y desencriptar documentos digitales. Si un documento se encripta con una llave, solo puede ser desencriptado con su par. Son ejemplos de algoritmos de llave pública Rivest, Shamir, Adelman (RSA) y algoritmos de curvas elípticas.[4]

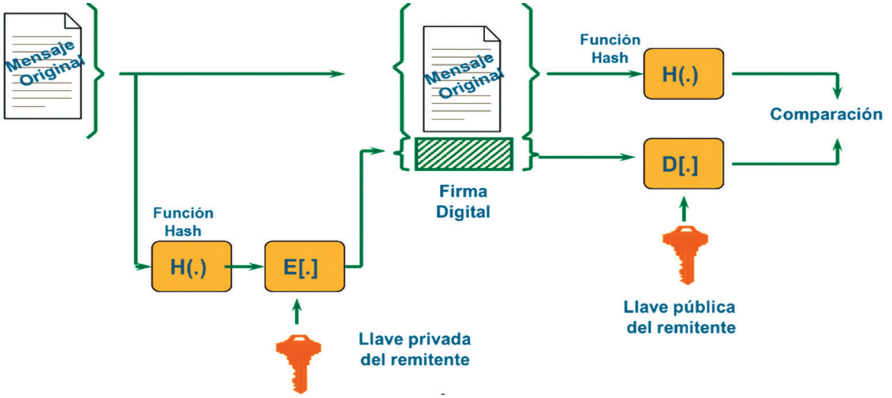
Cuando un usuario quiere utilizar algoritmos de llave pública para encriptar un documento o firmarlo digitalmente, se genera un par de llaves. Una, la llave pública, se da a conocer a todos, mientras que la otra, la llave privada, solo es conocida por el propietario de las llaves. Encriptar un documento con estos algoritmos es costoso en términos de cómputo, por lo que en general se prefiere firmarlo en lugar de encriptarlo completamente.[5] El proceso funciona como se muestra en la figura 1.

1. Se genera un compendio digital del documento a través de una función *hash* criptográfica. Como se explicará adelante, este compendio es muy pequeño (por ejemplo, en el *blockchain* de *bitcoin* solamente es de 32 bytes) y puede ser considerado como una huella digital del documento original.
2. El compendio se encripta con la llave privada del remitente. Esta es la firma digital que se le añadirá al documento original y se enviará al destinatario.
3. Cuando se recibe el documento, se desencripta la firma digital con la llave pública del remitente para obtener el compendio original y al mismo tiempo se vuelve a calcular el compendio del documento recibido.

[4] William Stallings, *Cryptography and network security: Principles and practices*, 2005, Nueva Jersey, Prentice Hall, 2005.

[5] Andrew S. Tanenbaum y David J. Wetherall, *Computer networks*, 2010, Boston, Pearson.

FIGURA 1
Cómo autentificar y mantener la integridad con una firma digital



En este procedimiento, si los dos compendios coinciden, se garantiza la integridad y la autenticidad del documento enviado. La integridad, porque si se altera el mensaje original, el compendio recalculado sería diferente del que se encuentra en la firma digital recibida; y la autenticidad, porque si el compendio desencriptado de la firma digital es igual al recalculado, se puede garantizar que el documento fue firmado por el emisor, quien no puede negar haberlo enviado.

Los algoritmos de llave pública también pueden proporcionar confidencialidad. Para esto, se encripta el documento con la llave pública del destinatario, de tal manera que solo él pueda desencriptarlo con su llave privada.

En el entorno de *bitcoin* se utilizan algoritmos de llave pública para proteger las transacciones. Sin entrar en detalles técnicos, en una transacción enviada a una persona cualquiera, digamos José, el emisor firma con la llave pública de él. De esta manera, solo José puede desencriptar la transacción con su llave privada y tomar posesión del activo intercambiado.

Función hash criptográfica

Una *función hash* (función de troceado) es un algoritmo matemático que transforma una cadena de bits de cualquier tamaño en una cadena de bits de un tamaño fijo determinado. Una función *hash* criptográfica es un caso especial de una función *hash*, cuyas propiedades son ideales para usos criptográficos, dado que están diseñadas de tal modo que no se pueda invertir la función.

Una función *hash* criptográfica tiene cinco propiedades principales: *1)* Es determinista, de tal modo que la misma cadena (o "mensaje") de entrada siempre resulta en el mismo compendio o "valor "; *2)* es fácil y rápido calcular el valor *hash* de cualquier mensaje; *3)* es computacionalmente imposible generar un mensaje de entrada dado su valor *hash*, y la única alternativa para encontrar un mensaje correspondiente a un valor *hash* particular es enumerar todos los posibles mensajes; *4)* un cambio pequeño en el mensaje produce un valor *hash* totalmente distinto; *5)* es "casi imposible" encontrar dos mensajes diferentes con el mismo valor *hash*.

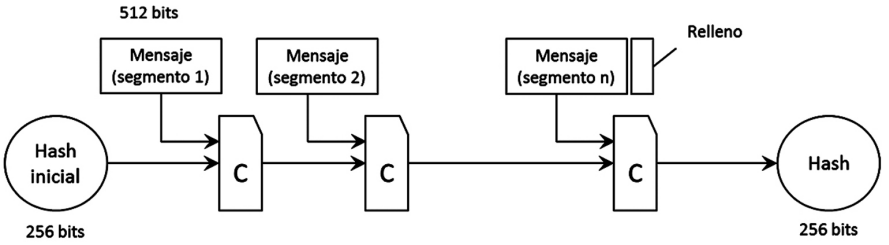
Una de las funciones *hash* criptográficas más utilizadas es SHA-256, desarrollada por la Agencia de Seguridad Nacional estadounidense. Esta función se utiliza en el entorno de *bitcoin* así como en otras aplicaciones de *blockchain*. En la figura 2 se muestra cómo opera la función:

1. Se separa el mensaje de entrada en varios segmentos de tamaño predeterminado. La cadena de bits (unos y ceros) que representa el contenido digital de cualquier tipo (por ejemplo, texto, video o una transacción digital) se divide en bloques de 512 bits. Cuando el tamaño original no es un múltiplo de 512, se completa (o rellena) el último bloque con bits de valor 0. Por ejemplo, un mensaje de 5220 bits se divide en 11 bloques: 10 de 512 bits y el último con los 100 bits restantes y 412 bits 0 de relleno.
2. Se toma el bloque 1 y un valor inicial de 256 bits definido por la norma[6] como entrada para la función de compresión C para producir la salida 1, de 256 bits.

[6] Secure Hash Standard, FIPS PUB 180-4, National Institute of Standards and Technology, marzo de 2012.

3. Se introducen el bloque 2 y la salida 1 a la misma función de compresión C para producir la salida 2 de 256 bits.
4. Se repite el paso tres hasta que se introducen el último bloque y la salida anterior a la función C. Por ejemplo, en un mensaje de 5220 bits se repetiría el paso tres hasta que se introduzca el bloque 11 y se obtenga la salida 10. Esta última salida es el valor *hash* deseado.

FIGURA 2
La función *hash* criptográfica SHA-256.[7]



Cómo funciona el *blockchain* del *bitcoin*

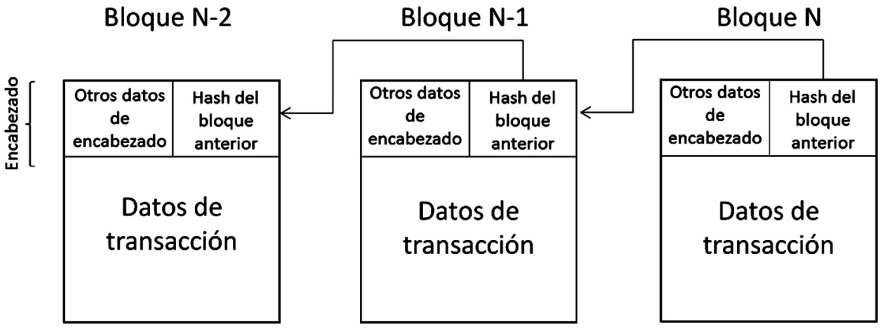
Blockchain y apuntadores hash

En el ecosistema de *bitcoin*, las transacciones (es decir, una trasferencia de *bitcoins* de un usuario a otro) se agrupan en bloques creados periódicamente. Cada bloque se identifica de forma única por un valor *hash* de su encabezado, que a su vez está compuesto por varios elementos incluyendo un valor *hash* obtenido a partir del contenido del bloque. El encabezado también almacena el valor *hash* del bloque pasado.[8] Por lo tanto, el nuevo bloque "apunta" al anterior, como se muestra en la figura 3.

[7] Edward Felten y Arwid Narayanan, "Introduction to crypto and cryptocurrencies", Coursera, University of Princeton, 2015.

[8] Como veremos en la siguiente sección, no es estrictamente cierto, puesto que algunos bloques pueden ser creados en paralelo.

FIGURA 3
Estructura de una *blockchain*[9]



La idea de tener valores *hash* "apuntando" a bloques anteriores es lo que llevó al concepto de un *blockchain*. Un bloque está "encadenado" al bloque cuyo valor *hash* está en su encabezado formando una "cadena de bloques", un *blockchain*. Esta estructura hace que sea imposible realizar cambios a la información o los encabezados de los bloques sin ser descubierto. Por ejemplo, si un hacker (pirata informático) altera la información del bloque N-2 de la secuencia, donde N es el tamaño actual del *blockchain*, el apuntador *hash* del bloque N-1 ya no correspondería al valor *hash* del bloque N-2. Para pasar desapercibido, el hacker también tendría que modificar el apuntador *hash* del bloque N-1, pero esta acción haría que a su vez el valor *hash* del bloque N que apunta al bloque N-1 difiriera del valor del bloque N-1. Al final, el hacker tendría que seguir alterando los apuntadores *hash* de la cadena hasta llegar al final (bloque N). Ahora bien, si se altera el contenido del bloque N, el valor *hash* almacenado en el apuntador H que apunta hacia el bloque N no coincidiría con el valor *hash* del bloque alterado N, por lo que se revelaría el intento del hacker.

Algunos lectores meticulosos se preguntarán: ¿y cuál es el problema? Si es fácil calcular funciones *hash* en computadora, ¿por qué no se podrían modificar todos los valores *hash* que fueran necesarios? La respuesta es que resultaría inviable. Como se verá adelante, el *blockchain* tiene un mecanismo de prueba de trabajo (*proof-of-work*) que vuelve muy

[9] Felten y Narayanan, *op. cit.*

costoso en términos de cómputo modificar los valores *hash* del *blockchain*. Los valores *hash* del *blockchain* no pueden tener cualquier valor, sino que están restringidos por ciertas condiciones.

Otro factor que hay que considerar es que un *blockchain* es, de hecho, una base de datos repetida. El número de copias del *blockchain* almacenadas simultáneamente en distintos repositorios puede ser enorme; por lo tanto, aun cuando se pueda alterar una instancia del *blockchain*, esta sería rechazada por la mayoría de los jugadores en el ecosistema.

Un *blockchain* emula digitalmente una de las características más importantes de los tradicionales libros de contabilidad en papel: una vez que se asienta ahí una transacción, es casi imposible modificarla.

Evitar el doble gasto: El consenso implícito

En principio, las criptomonedas son objetos digitales intangibles que se copian fácilmente, de la misma manera que casi todo el contenido digital. Por lo tanto, uno de los principales problemas de las criptomonedas antes de la aparición del *blockchain* de *bitcoin* era cómo evitar el doble gasto de la misma moneda sin la necesidad de una autoridad de confianza central que llevara control de todas las transacciones. En *bitcoin* y otras aplicaciones de *blockchain*, el problema se resuelve con un mecanismo de consenso implícito integrado a las reglas que gobiernan el ecosistema completo.

El consenso implícito funciona de la siguiente manera. Supóngase que Juan quiere transferir una cantidad determinada de *bitcoins* a José. Para esto, Juan crea y firma digitalmente una nueva transacción a nombre de la identidad digital de José (que está relacionada con la llave pública de José), la cual queda almacenada en un bloque del *blockchain*. Esta transacción se envía por internet a varios nodos del *blockchain*. Cada uno de estos nodos, conocidos como "mineros", es un sistema de cómputo con el *software* del *blockchain* que le permite buscar nuevas transacciones para añadir al *blockchain*, y que además compite con los demás nodos para ser el elegido y agregar un nuevo bloque con estas transacciones a la cadena.

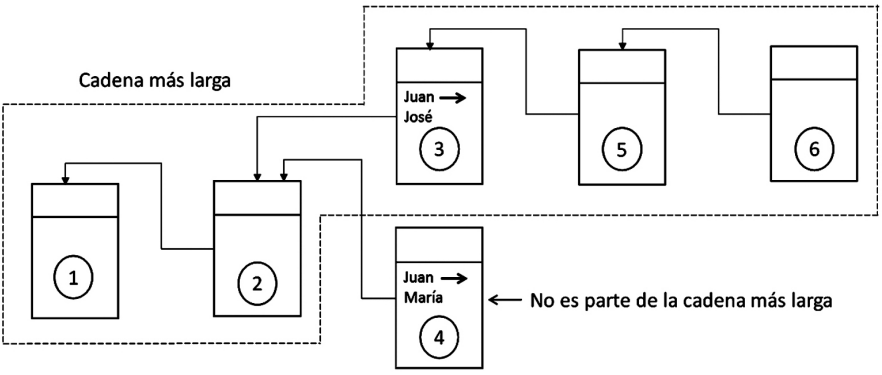
Ahora veamos qué sucedería si Juan quisiera engañar al sistema y envía una segunda transacción en la que transfiere los mismos *bitcoins*,

pero ahora a nombre de otra persona, por ejemplo María. Esta transacción sería parte de un nuevo bloque que será agregado al *blockchain*. Si el bloque con la transacción de Juan a José ya fue añadido a la cadena, cualquier minero detectará que Juan está tratando de hacer un doble gasto de los mismos *bitcoins* y, por lo tanto, invalidará la transacción.

Ahora supongamos que ambos bloques, el que contiene la transferencia de *bitcoins* de Juan a José (digamos, el bloque 3) y el que contiene la transferencia de *bitcoins* de Juan a María (digamos, el bloque 4) no se crean en secuencia, sino en paralelo, con distintos mineros que tratan de añadirlos al *blockchain* como se muestra en la figura 4. En este caso, uno de los dos bloques (el bloque 3 o el bloque 4) se considerará inválido, ya que se añadirán bloques nuevos al bloque 3 o al bloque 4. Con el tiempo, un bloque solo se considera válido si es parte de la cadena más larga. Vale la pena observar que la transacción válida puede terminar siendo la transacción con José o la transacción con María. El *blockchain* solo garantiza que se evite el doble gasto, pero no indica cuál de las dos transacciones será válida al final.

Los mineros reciben un incentivo solo cuando el bloque que agregan forma parte de la cadena más larga. Esto implica que otros mineros validan implícitamente los bloques añadidos antes al extender el *blockchain* a partir de ellos; de allí el nombre de "consenso implícito".

FIGURA 4
Un intento de doble gasto



Proof-of-work (prueba de trabajo) e incentivos

Los mineros compiten unos con otros al resolver un rompecabezas criptográfico. Para esto, se trata de encontrar una cadena de bits que, cuando se utiliza como entrada de determinada función *hash* criptográfica, produce un resultado predefinido. Como la única manera de encontrar la respuesta a este acertijo es probar diferentes cadenas de bits hasta encontrar la correcta, los mineros con mayor poder de cómputo tienen una mayor probabilidad de ganar el derecho de agregar un nuevo bloque al *blockchain*. El primer minero en ganar agrega el nuevo bloque a la cadena, y cuando se añaden más bloques, se le paga un incentivo por haberlo creado.[10] Usualmente, los mineros también reciben una comisión por cada transacción que se agrega a un bloque que finalmente se convierte en parte del *blockchain*.

Cuando un minero da comienzo a la creación de un bloque, empieza a resolver el problema criptográfico, el cual se considera como una "prueba de trabajo" (*proof-of-work*). En la mayoría de las aplicaciones del *blockchain*, el rompecabezas consiste en encontrar un *nonce* (es decir, un número usado solo una vez) que, cuando se agrega al encabezado del bloque, da como resultado un valor *hash* del bloque que es menor que el objetivo de dificultad definido en el encabezado del bloque. En términos simples, se dice que "minar" es el proceso de probar múltiples *nonces*, uno a la vez, hasta encontrar uno cuyo valor *hash* resultante sea menor que el objetivo específico. Como no se puede determinar de antemano el valor de una función *hash*, y además es imposible identificar un patrón para producir un valor *hash* determinado, la única forma de producir un resultado que coincida con un objetivo específico es intentar una y otra vez, al azar, diferentes *nonces* hasta que uno de ellos, combinado con los demás campos del encabezado del bloque, cumpla la restricción de que el valor *hash* resultante sea menor que el objetivo de dificultad.

Cabe notar que, aunque encontrar un *nonce* que resuelva el rompecabezas es muy difícil e implica mucho poder de cómputo, validar que

[10] De hecho, en el ecosistema de *bitcoin*, esta es la única forma de crear nuevos *bitcoins*. En agosto de 2017, cada vez que un minero añadía un bloque válido al *blockchain* recibía 12.5 bitcoines.

el acertijo fue resuelto correctamente es una tarea que puede hacer cualquier otro nodo. Basta calcular el valor *hash* y verificar que sea menor al objetivo de dificultad.

En ecosistemas como el de *bitcoin*, los mineros resuelven la prueba de trabajo utilizando *hardware* especializado, por ejemplo, los circuitos integrados de aplicación específica (*application specific integrated circuits, ASIC*), en los que cientos de miles de circuitos integrados corren el algoritmo de SHA-256 en paralelo a velocidades altas. Además, hay grupos de mineros que colaboran para resolver los acertijos y compartir las recompensas.

Como el *hardware* evoluciona rápidamente, el objetivo de dificultad se recalcula periódicamente, de manera que el tiempo para resolver el rompecabezas permanezca constante. En el ecosistema de *bitcoin*, cada 2016 bloques se calcula automáticamente un nuevo objetivo de dificultad. Todos los nodos recalculan la dificultad comparando los actuales tiempos de resolución del problema con el tiempo deseado, que es de 10 minutos en el entorno de *bitcoin*.

Una vez que un minero encuentra el *nonce* que resuelve el acertijo, inmediatamente transmite el bloque recién creado a sus pares. Estos pares verificarán la validez del bloque y, si es válido, lo transmiten igual que en las transacciones que se propagan a todos los nodos de la red. A medida que el bloque se propaga, cada minero recibe el nuevo bloque, lo añade y extiende a su propia copia del *blockchain*. De esta manera, la base de datos distribuida se actualiza automáticamente.

Blockchain: ¿El protocolo de confianza?

Durante décadas se han realizado esfuerzos para resolver mediante criptografía los problemas de privacidad, seguridad e inclusión de las criptomonedas. *Blockchain*, la tecnología de cadena de bloques detrás del *bitcoin* garantiza integridad (ya que las transacciones están firmadas) y transparencia (pues se trata de una base de datos distribuida) sin la necesidad de un tercero de confianza (debido al consenso implícito). Esto tiene grandes implicaciones para el sector financiero y para la sociedad en general.

Esta especie de "libro mayor" puede emplearse para registrar o intercambiar cualesquiera activos importantes o valiosos, como certificados de nacimiento, títulos de propiedad, votos, transferencias de dinero, contratos inteligentes y otros. De hecho, algunas empresas están utilizando el *blockchain* de *bitcoin* como una forma de almacenar información que no tiene nada que ver con la moneda.

Don Tapscott considera que la tecnología de *blockchain* será la tecnología que permitirá una "verdadera economía de intercambio entre pares".[11] Hoy en día, muchas compañías han desarrollado modelos de negocio que permiten compartir activos entre las personas. Por ejemplo, Uber permite compartir automóviles y Airbnb permite compartir viviendas. Sin embargo, ambas compañías centralizan su operación y la información de sus correspondientes negocios. En el futuro, uno podría pensar en usuarios compartiendo sus activos sin la necesidad de una compañía central entre ellos.

En palabras de Tapscott, "estamos emigrando de un internet de colaboración, eficiencia de búsqueda, acopio de datos y toma de decisiones en el que el punto central era monitorear, mediar y monetizar información y transacciones, a un internet de menores costos de negociación y contratos comerciales y sociales, en el que se dará la preponderancia a la integridad, seguridad, colaboración, privacidad y creación y distribución de valor".[12]

[11] Tapscott y Tapscott, *op. cit.*
[12] *Loc. cit*.