Facultad de Ciencias Económicas y Empresariales

APLICACIÓN DE LA TECNOLOGÍA BLOCKCHAIN EN LA IDENTIDAD DIGITAL

Autor: Agustín Pérez Ferrándiz

Directora: Josefina Bengoechea Fernández

Madrid, junio de 2022

ÍNDICE

1. Introducción

1.1. Interés en el tema

En un contexto empresarial y tecnológico que avanza más rápido que nunca, hay una tecnología que resalta sobre el resto y que acapara la atención de empresas y personas. Se trata del Blockhain, tecnología introducida de forma práctica por primera vez en 2008 con el Bitcoin por Satoshi Nakamoto. Esta nueva tecnología basada en la criptografía, la transparencia y la descentralización evoluciona día a día. Las propiedades del Blockchain hacen que sea idóneo no sólo para las criptomonedas, si no también para muchos sectores en los que la seguridad y la transparencia son vitales. Plataformas como Ethereum permiten al Blockchain convertirse en una herramienta mucho más versátil y escalable, poniendo como límite para hallar nuevos usos la imaginación de las personas.

Otro de los temas del momento es el Big Data, toda la información que generamos los individuos en la red, información que es susceptible de malversación debido a su gran valor. Es por ello que la seguridad de esta información es un asunto cada vez más importante, pues con el avance de internet, cada vez generamos más información, más valiosa y más sensible.

1.2. Objetivos

El objetivo de este trabajo es dilucidar hasta que punto es viable aplicar la tecnología Blockchain a la gestión de la identidad digital de las personas. Primero estudiaremos en profundidad la tecnología Blockchain, su funcionamiento, variantes, tipos y categorías. Analizaremos los sistemas existentes de gestión de identidad, sus puntos flacos y veremos si las cadenas de bloques tienen capacidad para suplir las carencias actuales de los sistemas de gestión de identidad digital.

1.3. Metodología

Para cumplir el objetivo mencionado anteriormente, la metodología utilizada será la revisión bibliográfica sistemática. Existen tres razones principales para hacer uso de esta metodología:

1. Resumir la evidencia existente relativa a una tecnología.
2. Identificar lagunas durante la investigación para así sugerir áreas susceptibles de una
investigación más profunda.
3. Establecer un marco sobre el que posicionar nuevas investigaciones.

1.4. Palabras clave

- Token: Unidad de valor creada por una organización para gobernar su modelo de negocio y dar más poder a sus usuarios. Un ejemplo de token es el BTC (Bitcoin).

- Nodo: En una Blockchain un nodo es un punto de conexión a una red desde el que se puede crear, enviar y recibir información.

- P2P: Peer-to-peer, nombre que reciben las redes descentralizadas en las no existen autoridades centrales, por lo que las relaciones son de usuario a usuario. Los nodos son los puntos de conexión de estas redes P2P.

- DLT: Distributed Ledger Technology. Hace referencia a la descentralización de la información en una Blockchain. Cada nodo contiene una copia del libro de cuentas de la cadena, de ahí su nombre.

- Hash: Función criptográfica utilizada en las cadenas de bloques para garantizar la autenticidad y seguridad de la información.

- Nonce: Abreviación para “number only used once”. En criptografía es el número que deben hallar los mineros para hallar el hash objetivo y minar un nuevo bloque.

- Mecanismo de consenso: Protocolo utilizado en Blockchain para garantizar que los nodos están sincronizados entre sí.

- Identidad digital: Conjunto de información generada por una persona en internet y que complementa a su identidad física.

2. La tecnología Blockchain

Los últimos años, en especial desde 2017, hemos experimentado un "boom" espectacular de un nuevo concepto monetario: Las criptomonedas. Hoy la inmensa mayoría de las personas han oído hablar de ello, en especial del Bitcoin, primera criptomoneda introducida en el mercado en 2009. Sin embargo, mucha menos gente a oído hablar del sistema que sustenta el Bitcoin y que le da sentido, la tecnología Blockchain.

2.1. ¿Qué es el Blockchain?

Como he mencionado anteriormente, la tecnología Blockchain se popularizó enormemente a raíz de la introducción del Bitcoin en 2008 por Satoshi Nakamoto, pseudónimo utilizado por el creador o grupo de creadores de esta moneda digital, en un artículo llamado "*Bitcoin: A peer-to-peer electronic cash system"* (Nakamoto, 2008).

Satoshi Nakamoto concibió el concepto de moneda digital "Bitcoin" en 2008, basado en la tecnología Blockchain, que permite a sus usuarios realizar transacciones sin que estas necesiten ser revisadas y validadas por una tercera parte (Nakamoto, 2008). Este artículo describía una nueva forma de moneda digital cuyo valor residía en permitir el envío de dinero de un usuario a otro sin la necesidad de contar con una tercera parte confiable. Para conseguirlo, se valía del uso del Blockchain, que no es otra cosa que una base de datos que almacena un historial de transacciones que son distribuidas, validadas y mantenidas por una red de ordenadores distribuidos por todo el mundo (Sarmah, 2018).

En lugar de utilizar un banco central para validar las transacciones, estas son supervisadas por toda la comunidad y ningún individuo tiene poder sobre esa base de datos, ni poder de cambiar o modificar esas entradas, ya que ese cambio debe ser ratificado por la mitad más uno de la red de usuarios. En otras palabras, si una base de datos está centralizada en un servidor único, el Blockchain es distribuido entre los usuarios. El Blockchain permite a cualquier usuario ver las transacciones de cualquier otro usuario, haciendo imposible para una entidad central hacerse con el control de la red (Sarmah, 2018). El sistema Bitcoin ordena las transacciones almacenándolas en bloques

que son ligados unos a otros mediante lo que llamamos Blockchain. Estos bloques son unidos unos a otros de forma linear, en orden cronológico, cada bloque conteniendo el *hash* del bloque previo (Kikitamara, 2017).

La descentralización es la principal característica del blockchain, permitiendo que la información sea almacenada por todos los nodos de la red simultáneamente, en lugar de en una localización centralizada (Wadhwa, 2019). Las principales características de la tecnología blockchain son la seguridad, las marcas de tiempo, criptografía y la dificultad para alterar la información en ella contenida, puesto que la creación y la modificación de la información se basa en el consenso de los usuarios y debe ser aprobada por la mayoría de los nodos de la red (Swan, 2015).

2.2. Historia de la tecnología Blockchain.

La tecnología Blockchain como tal fue ideada por primera vez en 1991 por Stuart Haber y W. Scott Stornetta, quienes buscaban introducir una solución práctica para "sellar" documentos y de esta forma impedir que fueran falsificados o alterados. El sistema consistía en "una cadena de bloques protegida criptográficamente en la que nadie podía manipular las marcas de tiempo de los documentos" (Rodríguez, 2018).

Al año siguiente los merkle trees fueron incorporados en el diseño, permitiendo así el almacenamiento de más información en cada bloque. Lo que se consigue con esto es crear una cadena segura de bloques, cada bloque conteniendo la información del bloque anterior (en forma del hash del bloque anterior) más la información de todas las transacciones almacenadas en el bloque presente, pues contiene el "root hash" o top hash, como dice en la imagen (Java T Point, s.f).

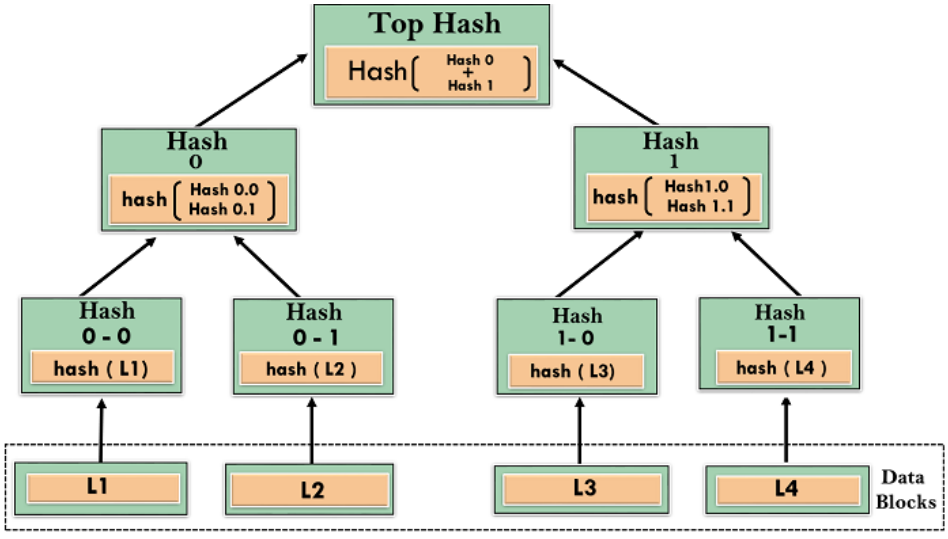

Imagen 1: Representación de una cadena de bloques con árboles de Merkle (Java T Point, s.f.)

El uso de los merkle trees es una parte vital de la tecnología Blockchain, pues como hemos dicho antes permite almacenar varias transacciones en un mismo bloque. La estructura de un bloque se entiende mejor en la siguiente imagen:

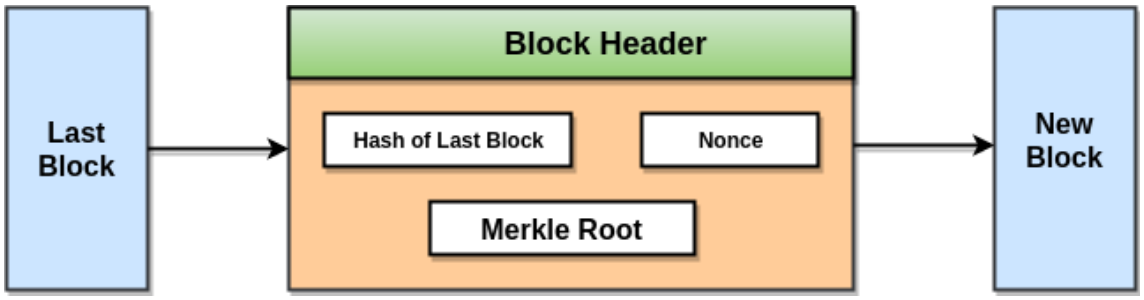

Imagen 2: Estructura de un bloque (Java T Point, s.f.)

En la imagen superior vemos como cada bloque de la cadena se compone del hash del bloque anterior, del *nonce* y el *root hash* de todas las transacciones del bloque. De esta forma, tener la merkle root o root hash en el bloque hace que la transacción sea inalterable. Como esa root hash contiene todos los hashes de cada una de las transacciones del bloque, se ahorra espacio y permite que el bloque contenga más de una transacción (Java T Point, s.f.).

Siendo esta la base principal sobre la que opera la tecnología Blockchain, no fue hasta 2008 con la conceptualización del Bitcoin cuando se materializó por primera vez la tecnología de forma exitosa. Cabe destacar que al contrario de lo que piensa mucha gente, el Bitcoin no fue la primera moneda digital, si no que ha habido muchas otras antes, aunque la primera en prosperar si que ha sido el Bitcoin, debido precisamente a la implementación del Blockchain.

A partir de aquí la tecnología se ha ido diversificando a medida que los usuarios han dio encontrando nuevos usos para ella. Podemos clasificar Blockchain en 4 categorías o niveles, dependiendo de para qué se use.

2.3. Categorías de Blockchain

Por motivos de organización y conveniencia, los diferentes usos y posibilidades dentro de la nueva revolución del Blockchain pueden ser divididos en 3 categorías: Blockchain 1.0, Blockchain 2.0 y Blockchain 3.0 (Swan, 2015).

2.3.1. Blockchain 1.0: Criptomonedas

Esta categoría nació en 2009 con el primer Bitcoin, y bajo ella agrupamos a todas las criptomonedas. Estas Blockchain se usa exclusivamente para criptomonedas. Antes de continuar debemos aclarar un concepto: La terminología Bitcoin puede llegar a ser confusa, ya que hace alusión a tres cosas diferentes. La primera es que Bitcoin se refiere a la plataforma Blockchain subyacente. En segundo lugar utilizamos la palabra Bitcoin para referirnos al protocolo que opera sobre esta tecnología Blockchain para describir como los activos son transferidos en la Blockchain. Por último, utilizamos Bitcoin para nombrar a la propia criptomoneda Bitcoin (Swan, 2015). La siguiente tabla ejemplifica de manera más clara lo que aquí hemos explicado.

Cryptocurrency: Bitcoin (BTC), Litecoin, Dogecoin
Bitcoin protocol and client: Software programs that conduct transactions
Bitcoin blockchain: Underlying decentralized ledger

Imagen 3: Capas en la tecnología Blockchain de Bitcoin (Swan, 2015)

Esta es la estructura utilizada por cualquier criptomoneda actual: Blockchain, protocolo y divisa. Una criptomoneda tiene normalmente su divisa y su protocolo, y puede operar en su propia Blockchain independiente o hacerlo en la Blockchain de Bitcoin. Por ejemplo, la criptomoneda Litecoin opera en el protocolo Litecoin, que opera en la Blockchain de Litecoin. Esto significa que Litecoin tiene su propio DL o libro de cuentas descentralizado, en la misma estructura y formato que la DLT de Bitcoin (Swan, 2015).

2.3.1.1. El problema del double spending y los generales bizantinos

El Bitcoin es la solución a un problema inherente al dinero electrónico, el double spending o doble gasto (no confundamos dinero electrónico con criptomonedas, pues el dinero de una cuenta bancaria gastado con una tarjeta de crédito es también dinero digital). El doble gasto consiste en enviar los mismos fondos a dos destinatarios distintos al mismo tiempo. Antes de la irrupción del Blockchain no había forma de comprobar que un lote de transacciones electrónicas no había ocurrido previamente sin un intermediario (banco). Estos intermediarios mantienen un libro de cuentas que confirma que cada lote ha sido gastado una única vez (Swan, 2015). Pero el contar con una entidad financiera que haga de intermediario no soluciona de todo el problema, pues sigue siendo posible falsificar billetes por ejemplo, o falsear cuentas bancarias. Pero en una Blockchain es imposible modificar una transacción que ya ha sido registrada.

Sin embargo, al solucionar el tema del doble gasto surge otro problema: El dilema de los generales bizantinos. La analogía es la siguiente: Imaginemos que tenemos que conquistar una gran ciudad, pero resulta imposible conseguirlo sin atacarla simúltaneamente por varios flancos. Entonces los dos generales se ponen de acuerdo, dividen el ejército en dos y se disponen a atacar la ciudad por dos puntos distintos a la vez. La clave de la victoria reside en comenzar el ataque exactamente al mismo tiempo en ambos puntos, ¿Pero como conseguimos esto? Sin una comunicación digital es muy difícil para los generales ponerse de acuerdo en cuándo atacar, y si estos se deciden a utilizar un mensajero para coordinar el ataque, no serían capaces de confiar en él, pues el ejército enemigo podría capturarlo y hacer que engañara a los generales, haciendo que fracasara el ataque. Entonces, ¿Hay alguna forma de autenticar el mensaje sin confiar en el mensajero?

Las cadenas de bloques también solucionan este problema combinando la tecnología peer-to-peer y la criptografía de la llave pública para crear una nueva forma de dinero digital (Swan, 2015). La posesión de la criptomoneda es registrada en el public ledger y confirmada por los protocolos criptográficos y por los mineros. De esta forma no es necesario confiar en ningún intermediario, aunque sí en el sistema (Swan, 2015).

Las distintas blockchain de esta categoría están pensadas para realizar transacciones de alta seguridad, anónimas y usuario a usuario, en divisas que no son propiedad de una entidad central (Mendoza, 2020).

2.3.2. Blockchain 2.0: Contratos

El Blockchain 2.0 se refiere al abanico conformado por todos las operaciones financieras, económicas y mercantiles que se valen del Blockchain y que son más complejas que simples transacciones monetarias: Acciones, bonos, futuros, créditos, hipotecas, títulos, propiedades inteligentes y contratos inteligentes (Swan, 2015).

Esta segunda categoría de Blockchain surge a raíz del desarrollo de Ethereum por Vitalik Buterin en 2013, que fue el primero en visualizar la escalabilidad de Bitcoin. Para comprender correctamente la diferencia entre el Blockchain 1.0 y el 2.0 debemos entender primero qué es Ethereum y en qué se diferencia su Blockchain de la de Bitcoin.

> Ethereum es software open source accesible a todos con el cual se crea una red de ordenadores descentralizados y conectados que integra una máquina virtual en todos estos equipos (nodos) para que la red pueda también ejecutar código de forma descentralizada. Estos programas se llaman smart contracts. (Caballero et al, p.173)

Una metáfora interesante acerca del Blockchain 2.0 es la del protocolo de la web. Al igual que una vez que la infraestructura y la tecnología de internet estaba asentada, se pudo empezar a construir nuevos servicios y funcionalidades sobre ella, como por ejemplo Amazon, o Netflix (Swan, 2015). De igual manera el Blockchain 1.0 sirve de base para ir construyendo encima protocolos 2.0.

De esta forma vemos que la principal diferencia entre las Blockchain 1.0 y las Blockchain 2.0 radica en que las segundas son capaces de programar código valiéndose de una red de ordenadores descentralizados, en lugar de en unos servidores centrales. Con ello, las Blockchain de segunda generación son capaces de programar smart contracts y con ellos dapps o aplicaciones descentralizadas (Caballero et al, 2020).

Simplificando, las Blockchain 2.0 permiten al usuario infinitas posibilidades de programación, cualquiera puede programar absolutamente cualquier cosa, y los bloques de la Blockchain de Ethereum no sólo pueden almacenar transacciones, si no también

estos smart contracts. Debemos aclarar que el término smart contract ni es un contrato ni es inteligente, si no que "hace referencia a un programa computacional inmutable que se ejecuta de forma determinista a través de la Ethereum Virtual Machine de cada nodo de la red Ethereum" (Caballero et al, 2020, p. 174). Como estos contratos no se almacenan en un servidor central si no que lo hacen en la Blockchain, estos no pueden cambiarse. En definitiva, Ethereum es la versión programable de Bitcoin. Quiero aclarar que existan otras muchas Blockchain 2.0 aparte de Ethereum, pero hago hincapié en esta última porque es la más extendida y sobre la que se basa la gran mayoría de los smart contracts.

2.3.3. Blockchain 3.0. Aplicaciones

El Blockchain 3.0 son todas los usos que se le pueden dar al Blockchain más allá de las finanzas, los mercados y las divisas, particularmente aquellas áreas relacionadas con el sector público, la salud, ciencia, cultura y arte (Swan, 2015). Las Dapps, como se menciona en el párrafo anterior, son aplicaciones como cualquier otra, con el matiz de que han sido programadas con una Blockchain y toda la lógica del back end se almacena en la propia Blockchain de forma descentralizada en lugar de en un servidor central como ocurriría con una aplicación del Appstore por ejemplo.

Esta categoría de Blockchain aún se encuentra en un estado de desarrollo temprano, aunque ya podemos vislumbrar el potencial y los distintos usos que puede llegar a tener. Sin embargo, las posibilidades de aplicación del Blockchain en esta categoría son tan dispares que lo más probable no es que haya una única cadena de bloques para todas las aplicaciones, si no que esta se diversifique y nos encontremos con una amalgama de Blockchains dispares entre sí, cada una líder dentro del sector para el que ha sido específicamente concebida (Mendoza, 2020).

El Blockchain 3.0 no se entiende sin las limitaciones actuales del Blockchain. Por así decirlo, el Blockchain 3.0 son las soluciones a las que se llegarán en un futuro para sortear los impedimentos que hoy limitan la escalabilidad del Blockchain (fundamentalmente velocidad de procesado). De esto hablaremos más adelante.

2.4. Tipos de Blockchain

Mientras que la sección anterior trataba sobre las distintas categorías entre las que podemos clasificar las cadenas de bloques por sus aplicaciones, en esta sección analizaremos los tipos de Blockchain que existen en la actualidad.

Existen cuatro tipos de cadenas de bloques en la actualidad: Públicas, privadas, de consorcio e híbridas. Lo que define a qué tipo pertenece cada una son las necesidades de la entidad que crea la Blockchain. Estos cuatro tipos pueden caracterizarse en restringidas, no restringidas o ambas. Las restringidas permiten a cualquier usuario unirse a ella anónimamente (esto es convertirse en un nodo) y no restringen los derechos de dichos nodos. Por otra parte, las no restringidas limitan el acceso a ciertos nodos y pueden tambié restringir sus derechos. La identidad de los usuarios de una red no restringida es conocida por el resto de integrantes de la red (Wegrzyn y Wang, 2021).

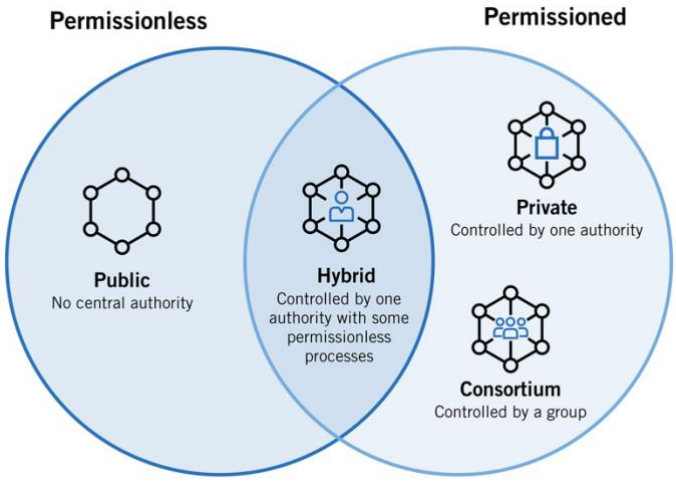

Imagen 4: Esquema de los distintos tipos Blockchain (Foley, 2021).

2.4.1. Blockchains públicas

Estas cadenas de bloques de basan en el principio de que cualquier persona del mundo puede acceder a la información contenida en ella. Cualquiera puede convertirse en un nodo de la red, validar transacciones y minar nuevos bloques. Estas Blockchain funcionan bajo la encriptación, algoritmos de consenso (como la Proof of Work (PoW) o prueba de trabajo y la Proof of Stake (PoS) o prueba de participación) y una serie de

incentivos económicos. La Blockchain pública más conocida es Bitcoin. Entre las ventajas de una Blockchain pública se encuentran:

- Seguridad. Las cadenas de bloques públicas son las más seguras, debido precisamente a que al ser públicas son con las que más usuarios cuentan, y por ende las más difíciles de hackear.
- Transparencia. Al ser públicas, cualquiera puede unirse a ella y ver las transacciones que en ella se realizan. Todo el mundo tiene una copia de su libro de cuentas y por ello nadie puede falsearlo.

2.4.1.1. Ejemplo, Bitcoin

Bitcoin es la criptomoneda por excelencia y fue la primera que entró en circulación bajo la tecnología Blockchain. Ha sido a partir de Bitcoin que se ha ido desarrollando la tecnología Blockchain. Bitcoin es una criptomoneda y sistema de pago digital en la que se usa la criptografía para regular la generación de nuevas Bitcoin y para verificar las transacciones sin necesidad de un banco central (Swan, 2015). Bajo la perspectiva de un usuario, los elementos de los que se compone Bitcoin a la hora de transaccionar son una clave dirección, una clave privada, una wallet y un ordenador (Swan, 2015).

2.4.2. Blockchains privadas

Una Blockchain privada es aquella cadena de bloques restringida que opera en una red cerrada. Normalmente estas son utilizadas en empresas u organizaciones privadas donde únicamente una serie de miembros seleccionados pueden participar en ella (Data-Flair, s.f.). Las principales ventajas de las Blockchains privadas son la velocidad y la escalabilidad. Al estar restringidas a unos cuantos nodos, la red es infinitamente más rápida que en el caso de las públicas, pues el consenso es mucho más ágil. También es mucho más rápido añadir bloques a la cadena y verificar las transacciones. En cuanto a la escalabilidad, las privadas tienen la ventaja de que pueden ser diseñadas a medida de una institución o empresa en concreto, lo que las dota de una flexibilidad que una Blockchain pública no tiene (Data-Flair, s.f.). La desventaja es una menor seguridad, ya que como hemos dicho, al no ser pública no todo el mundo puede unirse y al tener menos nodos es

más fácil de manipular. Los mejores ejemplos de Blockchain privadas son Multichain y Hyperledger.

2.4.2.1. Ejemplo, Multichain y Hyperledger

Multichain es una plataforma para crear y desplegar Blockchains privadas. Soluciona los problemas relativos al minado, la privacidad y la apertura a través de la gestión privada de la restricción a usuarios (Greenspan, 2015). La principal ventaja para usuarios institucionales es que permite desarrollar y desplegar Blockchains privadas sin contar con desarrolladores especializados.

Hyperledger es un proyecto colaborativo respaldado por la Linux Foundation que busca facilitar la implementación de la tecnología Blockchain en el mundo empresarial, sin importar la industria a la que pertenezca la empresa (Hyperledger, s.f.).

2.4.3. Blockchains de consorcio

Las Blockchain de consorcio son Blockchains restringidas gobernadas por un grupo de organizaciones en lugar de una sola entidad. A diferencia de las privadas están semidescentralizadas, pues en lugar de estar gobernadas por una sola entidad lo están por un grupo de entidades. Más de una entidad está habilitada para actuar como nodo, ralizar transacciones y minar bloques. Mantiene las mismas ventajas que una Blockchain privada, aunque es algo más segura (Data-Flair, s.f.).

2.4.3.1. Ejemplo, R3

R3 es una compañía de DLT con sede en Nueva York que se ha aliado con algunas de las entidades financieras más importantes del mundo con la misión de introducir los beneficios de los DLT en el sector financiero (Higgins, 2015).

2.4.4. Blockchains híbridas.

Una Blockchain híbrida es una mezcla entre una cadena de bloques privada y una pública en el sentido de que puede tener una red de acceso restringido y otra u otras sin

restringir dentro. Los usuarios necesitan permiso para unirse a la red privada, pero una vez dentro pueden acceder a la pública. La información contenida en la red privada normalmente se verifica dentro de ella, aunque si el usuario en concreto desea una verificación más fiable puede decidir colgarla en la pública (Data-Flair, s.f.). Un ejemplo de una Blockchain híbrida es IBM Food Trust, que se desarrolló para optimizar la eficiencia a lo largo de toda la cadena de suministro de la comida (Wegrzyn y Wang, 2021).

2.5. Arquitectura del Blockchain

Para comprender correctamente como funciona dinámicamente una cadena de bloques, primero tenemos que analizar sus diferentes partes. Dividiremos esta sección en estructura de los bloques, consenso, red descentralizada y firma digital.

2.5.1. Estructura de los bloques

En una red Blockchain, las transacciones generadas son validadas por los distintos nodos de la red y después son añadidas a un bloque, que no es otra cosa que una conjunción de distintas transacciones. Estas transacciones son las que conforman el cuerpo del bloque. Sin embargo, un bloque está dividido en dos, en el mencionado cuerpo, y en el block header.

2.5.1.1. Block header

El block header se utiliza para identificar un bloque concreto en una cadena, sería como una especie de matrícula. Cada bloque contiene un header único, y cada bloque es identificado por el hash de dicho header. Cada block header está compuesto de los siguientes elementos: El hash del bloque anterior, el número del bloque, una marca de tiempo, un nonce y el hash del merkle root. La merkle root es el root hash del merkle tree que se almacena en el cuerpo del bloque y que contiene todas las transacciones del bloque (Hayes, 2021).

2.5.1.1.1. Hash

Este es el elemento más importante del bloque, y es lo que permite la encriptación de toda la cadena. Un hash es una función matemática que convierte un input numérico de cualquier longitud en un output numérico de una longitud determinada y fija. Además, no podemos utilizar un hash para revertir la función para obtener el valor de entrada a través del valor de salida, pues son funciones unidireccionales (Frankenfield, 2022). Es imposible que un hash de el mismo valor de salida a dos valores de entrada distintos. Ese valor de salida es de una longitud fija, que en el caso de Bitcoin, que utiliza la función SHA-256 son 64 caracteres. No todas las Blockchain tienen por qué utilizar la misma función hash, pero nos centraremos en la función SHA-256 al ser la utilizada en Bitcoin.

Una función hash tiene tres propiedades principales:

- La función SHA-256 es determinista: Siempre obtendremos el mismo valor de salida si recalculamos la función con el mismo valor de entrada.
- La función es imposible de revertir: Nunca sabremos por adelantado el valor hash que obtendremos hasta que sea calculado.
- Si introducimos en la función dos valores mínimamente diferentes, el valor de salida cambiará drásticamente.

Por tanto, sólo habrá un valor válido para calcular el hash objetivo. Ese número es el que los mineros tratan de calcular para poder generar el nuevo hash y minar el bloque, con su consiguiente recompensa.

2.5.1.1.2. El nonce

En la función hash se meten una serie de variables para obtener el hash objetivo. Estas son el hash del bloque anterior, los datos del cuerpo del bloque, el número del bloque, la marca de tiempo y el nonce. Un minero conoce todos esos datos salvo el nonce, que significa “number only used once”. Este nonce es el número que deben hallar para generar el hash del nuevo bloque. Es el único dato del bloque que está diseñado para estar bajo nuestro control, pues todos los demás datos (hash anterior, número de bloque y datos) nos vienen ya dados y son producto de la propia cadena (Eremenko, 2018). Por ello, si alguien tratara de falsificar un bloque ya minado no podría, pues el más mínimo cambio

provocaría que los hashes calculados a partir de ese bloque fueran radicalmente distintos (Eremenko, 2018).

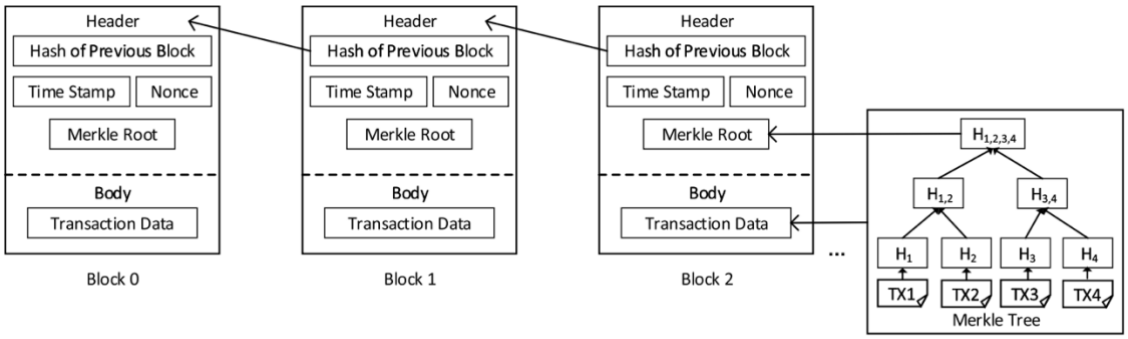

Imagen 5: Representación de la estructura de un bloque (Liang, 2020)

2.5.1.1.3. Merkle trees

Un merkle tree almacena todas las transacciones de un bloque produciendo una "huella dactilar" para todo ese conjunto de transacciones. Los merkle trees se crean calculando sistemáticamente pares de hashes hasta que solo queda uno, llamado root hash o merkle root (Java T Point, s.f.), que se almacena en el block header.

2.5.1.1.4. La marca de tiempo

En Bitcoin, la marca de tiempo es el número de segundos que han pasado desde el 1 de enero de 1970. Este número se incluye en cada bloque para hacer más difícil el minado, ya que a cada segundo que pasa el valor cambia. Como hemos dicho antes, el minero mete en la función SHA-256 el hash del bloque anterior, el número de bloque, la marca de tiempo, los datos del bloque y el nonce. Por ello, si la marca de tiempo cambia cada segundo, es mucho más difícil acertar con el hash requerido (Eremenko, 2018). Con el uso de las marcas de tiempo, todos los usuarios de la red sabrán además en que momento exacto se creó cada bloque, validando las transacciones en él contenidas.

2.5.1.1.5. Hash objetivo

El hash objetivo es utilizado para determinar el nivel de dificultad para minar nuevos bloques (Hayes, 2021). Dependiendo de la cantidad de mineros en la red, este nivel de dificultad va aumentando o disminuyendo para mantener el ritmo de nuevos bloques en una media de uno cada 10 minutos aproximadamente. El objetivo es un número de 256 bits que todos los usuarios de la red conocen y que como hemos dicho, va cambiando. El hash obtenido por un minero con la función SHA-256 debe ser igual o inferior al hash objetivo. Cuanto más bajo sea el objetivo, más difícil será calcularlo y generar un nuevo bloque (Bitcoinsv, s.f.).

Hay un total de 16^64 valores posibles para la función SHA-256, sin embargo, no todos ellos son válidos a la hora de minar un nuevo bloque. Esto es porque cada dos semanas Bitcoin genera un nuevo valor mínimo de hash para generar un nuevo bloque. Este valor es el hash objetivo al que los mineros deben llegar. Lo realmente importante en el hash objetivo es el número de ceros que haya antes del primer número distinto de cero, ya que determinará la magnitud del valor que deben calcular. Cada cero que haya antes reduce la magnitud del valor en un factor de 16. En el objetivo actual hay 18 ceros 000000000000000005d97dc00000000000000000000000000000000000000. Por tanto, si hay 18 ceros, 64 – 18 = 46. Por tanto 16^46 / 16^64 = 16^ (-18) = 0.000000000000000002%. Esta es la probabilidad de que un valor del nonce genere un hash válido para un nuevo bloque con el hash objetivo actual (Eremenko, 2018).

2.5.2. Red descentralizada

Las interacciones entre los usuarios de una Blockchain ocurren mediante una red descentralizada en la que cada usuario representa un nodo sobre el que el cliente de la Blockchain está instalado. Cuando un usuario realiza una transacción junto a otro usuario, o lo que es lo mismo, cuando un nodo recibe información de otro nodo, este verifica la autenticidad de los datos. Entonces transmite los datos validados al resto de nodos (Zheng, 2018). Con este mecanismo la información se transmite a través de toda la red. El beneficio de utilizar este sistema es que la centralización del factor humano es minimizada, y la confianza muta de los agentes humanos de una organización central a un código abierto (Atzori, 2015).

2.5.3. Consenso

Hemos visto que la tecnología consigue eliminar a las autoridades centrales en las transacciones, consiguiendo que estas sean completamente seguras y verificadas. Esto es únicamente posible gracias a los algoritmos de consenso, parte fundamental de la tecnología Blockchain (Patel, 2022). Un algoritmo de consenso es un procedimiento mediante el cual, todos los usuarios de la red llegan a un acuerdo común sobre el actual del distributed ledger. En esencia, lo que consigue el algoritmo de consenso es que cada uno de los bloques nuevos añadidos a la cadena sea la única versión válida y real del DL (Patel, 2022). Existen muchos algoritmos de consenso distintos, en realidad son casi infinitos, pues cada Blockchain puede diseñar el algoritmo que más le convenga. Sin embargo, la realidad nos muestra que son 4 los algoritmos de consenso que más se usan.

1. Proof of work (PoW)

   El PoW es el mecanismo más extendido y fue introducido con Bitcoin. El PoW hace referencia al mecanismo criptográfico que se basa en la capacidad de los usuarios de una red para resolver complejos problemas computacionales para conseguir una mayor participación en la red (Chaudhury, 2021). En el caso de Bitcoin, el mecanismo de consenso se llama Consenso de Nakamoto, que es un PoW llamado hashcash en conjunción con una serie de reglas. Consiste en que los mineros utilizan su poder computacional para competir entre sí y tratar de ser los primeros en resolver el problema computacional (siguiendo la función SHA-256, como explicamos anteriormente) para así poder minar el bloque y recibir la recompensa. Cuando el minero encuentra la solución al problema y mina el bloque, este se distribuye a toda la red donde es aprobado. Entonces recibe los Bitcoins correspondientes como recompensa a la electricidad gastada en dar con la solución (Chaudhury, 2021). Cuanto mayor poder computacional tenga un minero, más probabilidades tendrá de dar con la solución al hash del bloque.

   Este bloque sólo será validado si se cumple la “regla de la cadena más larga”. Esta regla consiste en que la cadena más larga de la red es la considerada válida porque es en la que más esfuerzo computacional se ha invertido y por tanto la que más trabajo de validación tiene (Nester, 2018). Estas reglas de validación se aseguran de que los bloques propuestos cuentan con el nivel requerido de trabajo computacional para poder ser aceptados por los validadores de la red. Si

el PoW no es válido, el resto de los nodos de la red ignorará el bloque inválido y no lo incluirán en sus cadenas. Esto impide que destinen sus recursos en la validación de una cadena inválida, y que empiecen a trabajar en la cadena "honesta" alternativa (Nester, 2018).

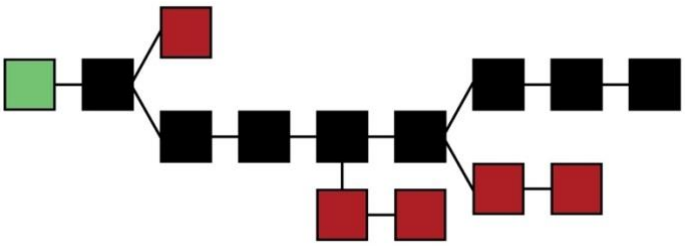

Imagen 6: Representación de la regla de la cadena más larga (Stone, 2018)

El PoW permite a la red de Bitcoin ser enteramente descentralizada y segura, ya que un usuario malicioso necesitaría el 51% de todo el poder computacional de la red para tomar el control y dar por válidos bloques ilegítimos, lo que es prácticamente imposible dado el tamaño de la red, aparte de que en caso de que se consiguiera, el Bitcoin perdería todo su valor y el ataque habría sido en vano. El PoW utilizado por Bitcoin se llama hashcash, y el utilizado por Ethereum Ethhash,

2. Proof of Stake (PoS)

Actualmente muchas cadenas están empezando a sustituir el PoW por el PoS, sobre todo debido a la enorme cantidad de energía que se consume con el PoW. El caso más relevante es el de Ethereum, que actualmente opera con PoW y está desarrollando ETH2, una nueva versión de la cadena que se basa en el PoS. En una Blockchain que utiliza PoS, el nodo que genere un bloque debe probar que tiene acceso a una cierta cantidad de monedas de esa red para poder ser aceptado (Pavel, 2015). Este método requiere que los validadores tengan un mínimo de monedas nativas "bloqueadas". Cuanto mayor sea el stake de un validador, menos probable será que ataque la red. El PoS alinea de forma natural los incentivos de los usuarios con el buen funcionamiento de la cadena (Xu et al, 2019). De esta forma sólo aquellos usuarios que tengan una cantidad mínima de monedas podrán

participar en el mantenimiento de la cadena. En el caso de Ethereum será necesario tener un stake de al menos 32 ETH para poder validar bloques.

Un validador es elegido para generar un bloque nuevo proporcionalmente a su participación de monedas. De esta forma, el consenso PoS incentiva a los validadores a llegar a un acuerdo mediante un mecanismo de recompensas (Patel, 2022). Al igual que en el PoW, hay muchos protocolos distintos para el PoS, cada uno diseñado para conseguir distintos objetivos favoreciendo unas propiedades sobre otras (Xu et al, 2019). Comparado con el PoW, PoS es mucho más eficiente en cuanto a costes, ya que requiere de mucho menos poder computacional para minar y la latencia es también menor (Xu et al, 2019).

3. Practical Byzantine Fault Tolerance (PBFT)

El mecanismo de consenso PBFT se emplea principalmente en cadenas restringidas. La principal cualidad del protocolo PBFT es que asegura el funcionamiento de la cadena aún cuando hay un cierto porcentaje de nodos bizantinos (se comportan de forma arbitraria). Dicho de forma simple, un consenso PBFT permite un novel de seguridad muy alto, con la contrapartida de que tiene una latencia bastante superior al resto de mecanismos de consenso, por lo que es difícil aplicarlo a redes no restringidas (Xu et al, 2019).

En un PBFT hay dos tipos de nodo, nodos primarios y de refuerzo. Un nodo de la red, actuando como cliente, emite transacciones como solicitud a un nodo primario y este decide el orden de ejecución de la solicitud. El nodo de refuerzo chequea la autenticidad de la solicitud, decide si ejecutarla o no y manda una respuesta al nodo cliente (Liang, 2020). El consenso de la transacción llega cuando el cliente recibe f+1 (siendo f el número de nodos bizantinos) respuestas de distintos nodos de refuerzo con el mismo resultado. El algoritmo PBFT garantiza la seguridad y el dinamismo de la red. Por ejemplo, una solicitud de un nodo cliente será respondida cuando haya menos de (n-1/3) nodos bizantinos, donde n es el número de nodos que participan en el proceso de consenso (Liang, 2020).

El consenso PBFT elimina el esfuerzo tan alto de computación de un PoW, pero requiere un alto nivel de confianza entre los nodos para resistir los ataques sybil (Douceur, 2002) donde un tercero malicioso crea un gran número de nodos para segar el consenso a su favor.

4. Delegated Proof of Stake (DPoS)

La diferencia entre PoS y DPoS es que mientras que el PoS es un mecanismo directamente democrático, el DPoS es representativamente democrático. Esto quiere decir que en el PoS el sistema asigna directamente a los validadores el derecho a minar un bloque aleatoriamente según cuantas monedas posean, mientras que en el DPoS son los stakeholders los que eligen los delegados para minar el bloque. La ventaja es que con un número de nodos para validar un bloque mucho menor, el proceso es significativamente más rápido (Zheng et al, 2018). El problema con este consenso es que requiere un cierto nivel de confianza en los delegados.

2.5.4. Solución de discrepancias

Puesto que una cadena de bloques se construye sobre una red descentralizada, puede llevar un tiempo que todos los nodos de la red actualicen y añadan un nuevo bloque. Además, hay un gran número de nodos minando al mismo tiempo, por lo que existe una probabilidad de que en el espacio de tiempo que se tarda en actualizar la cadena y añadir el bloque (este período recibe el nombre de latencia) se mine otro bloque. Esto da lugar a que puedan existir más de una cadena al mismo tiempo (Liang, 2020). En este supuesto es cuando surge una discrepancia. La discrepancia consiste lógicamente en que los nodos no saben cual de las dos cadenas es la válida y por lo tanto, sobre qué cadena trabajar. Como hemos explicado anteriormente, la discrepancia se soluciona aplicando la regla de la cadena más larga. La lógica tras esta regla es que la cadena más larga es en la que la mayoría de los nodos confían y sobre la que trabajan.

En el supuesto planteado anteriormente, donde dos bloques se crean y añaden a la cadena al mismo tiempo, lo que ocurriría es que los nodos se dividirían entre las dos cadenas, y tarde o temprano una de ellas sobrepasaría a la otra, momento en que la cadena

más corta quedaría invalidada. Todas las transacciones contenidas en la cadena corta volverían al memory pool o mempool (donde se almacenan las transacciones sin confirmar). Es por este problema que en Bitcoin por ejemplo se espera a que un bloque tenga 6 confirmaciones (que se hayan añadido 6 bloques más en la misma cadena) para que quede oficialmente confirmado y el minero reciba su recompensa.

2.5.5. Firma digital

Crear una nueva transacción en una Blockchain requiere el uso de una firma digital para autenticarla. Para verificar la autenticidad e integridad de la transacción las firmas digitales usadas en las cadenas de bloques se basan en la encriptación asimétrica. Cada nodo de la cadena tiene dos claves, una privada y una pública, y el contenido cifrado por una llave privada tan solo puede descifrarse con esa misma llave. Antes de que un nodo mande una transacción a la red, la cifra con la llave privada. El resto de los nodos pueden entonces verificar la transacción usando la llave pública. Con este sistema en que la clave privada es confidencial para su dueño, y la pública es conocida por todos los nodos, la veracidad de las transacciones es fácilmente contrastable (Liang, 2020).

Por ejemplo, si un usuario 1 quiere realizar una transacción, primero la firma generando un valor hash derivado de la propia transacción y cifrándolo, usando su llave privada. Entonces manda al usuario 2 el hash cifrado con la transacción. El usuario 2 la verifica mediante la comparación del hash descifrado (usando la llave pública del usuario 1) y el valor del hash derivado de la transacción recibida, utilizando la misma función hash que el usuario 1 (Zheng et al, 2018).

2.5.6. Funcionamiento del Blockchain

Para repasar el funcionamiento de una cadena de bloques, nos basaremos en una Blockchain que funcione con PoW, ya que es el mecanismo de consenso más extendido. En primer lugar, se inicia la transacción por un nodo y se transmite al resto de nodos en la red. Los nodos que reciben la transacción utilizan la firma digital para verificar la autenticidad de la transacción. Tras ser verificada, la transacción se añade a la lista de transacciones válidas en los nodos. Para registrar estas transacciones en la cadena, los nodos de la red trabajan para generar un nuevo bloque donde incluirlas, es decir se

esfuerzan en encontrar el nonce. El nodo que primero calcule el nonce válido será el que genere el nuevo bloque, que contendrá la transacción iniciada. El resto de los nodos verifican entonces las transacciones del nuevo bloque comparando la merkle root, y una vez que se comprueba que las transacciones del nuevo bloque son auténticas, el nuevo bloque se añade a la réplica local de la cadena (Liang, 2020). Es en este momento cuando la actualización de la cadena se da por completada.

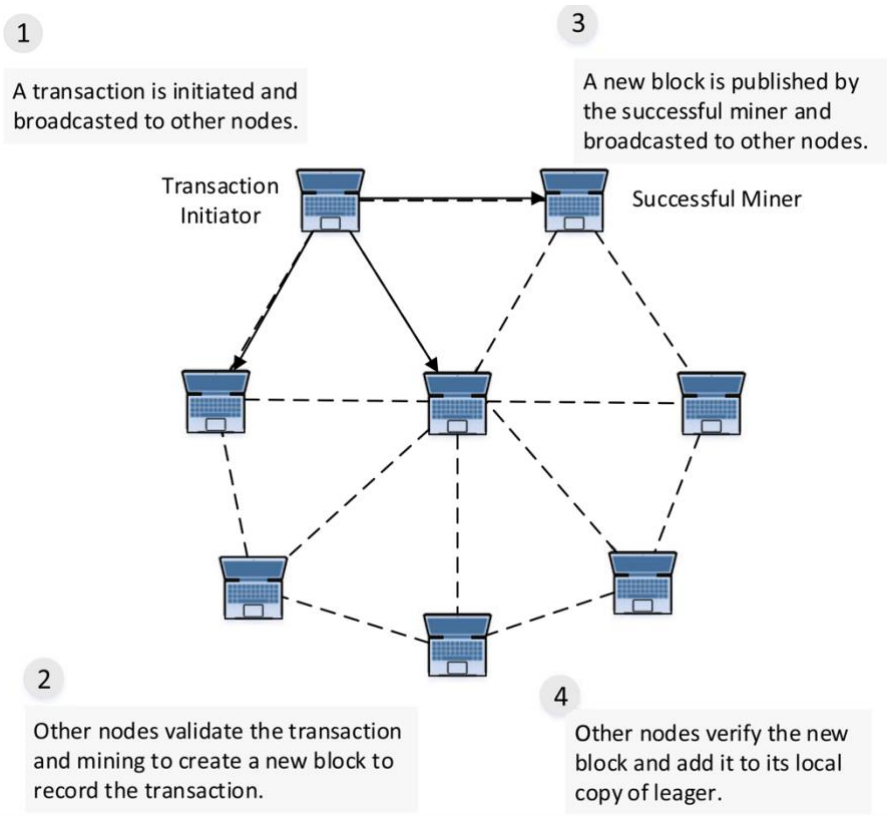

Imagen 7: Esquema del funcionamiento de una cadena de bloques (Liang, 2020)

2.6. Prestaciones fundamentales

En este capítulo estudiaremos las características que dotan a esta tecnología de la capacidad de implementarse en nuestras industrias, gobiernos y economías, y que explican la escalabilidad del Blockchain.

1. Eliminación de la necesidad de confiar en una tercera parte

La primera de estas características y que ya hemos tratado en profundidad es la capacidad del Blockchain de facilitar que dos o más entidades lleguen de forma segura a un acuerdo sobre una o unas acciones concretas a través de una red pública como internet sin contar con una tercera parte, como una oficina gubernamental o una entidad autorizadora (Al-Jaroodi et al, 2019).

2. Inmutabilidad

Uno de los factores clave en el éxito de Blockchain es la habilidad de proteger la información y las transacciones registradas en el DL usando una aproximación compartimentada y distribuida (Shrier et al, 2016). Este nivel de protección es posible gracias a distintos niveles de encriptación y la implementación de las funciones hash utilizadas por las cadenas de bloques. Además, la propia naturaleza de las cadenas de bloques hace prácticamente imposible la alteración de la información ya registrada en la cadena.

3. Descentralización

En una cadena de bloques pública, las transacciones (acciones) son registradas por todos los nodos de la red, y cada uno de ellos guarda una copia del DL en el que se registran. Así, el DL estaría protegido contra un hipotético fallo en un servidor central.

4. Imposibilidad de renegar

Una transacción se firma digitalmente con una llave privada antes de ser distribuida al resto de nodos. La autenticidad de las transacciones puede comprobarse por cualquiera con el uso de la clave pública, que está disponible para todo el mundo. Puesto que la clave privada sólo la tiene el dueño, este no puede luego renegar de la transacción.

5. Transparencia

En una Blockchain pública, todos los nodos pueden acceder a las transacciones contenidas en la cadena y verificar las nuevas. Por ello una Blockchain implica máxima transparencia.

6. Rastreabilidad

Los bloques de una cadena se añaden en orden cronológico y cada block header contiene su correspondiente marca de tiempo que indica el momento exacto en el que el bloque se creó. Por ello los nodos pueden fácilmente rastrear el origen de cualquier bloque.

2.6. Aplicaciones del Blockchain

Esta sección está estrechamente relacionada con el capítulo "categorías del Blockchain". En primera instancia el Blockchain se implementó única y exclusivamente en el ámbito financiero, concretamente con el desarrollo de las criptomonedas. Esto es lo que llamábamos Blockchain 1.0. Sin embargo, la comunidad no tardó en darse cuenta de las posibilidades tan amplias que ofrece esta tecnología, y rápidamente surgió lo que llamamos Blockchain 2.0, que como explicábamos es la implementación de Smart contrats en la cadena, ampliando enormemente las aplicaciones de la tecnología, que ya no se reducen al ámbito financiero, si no que puede implementarse prácticamente en cualquier sector o industria. Por último, hablamos del Blockchain 3.0 que está relacionado con el concepto Web 3. Esta última categoría se comprende como las evoluciones y variaciones que experimente la tecnología Blockchain en un futuro cercano, buscando solución a las limitaciones que tiene actualmente.

La implementación del Blockchain va a tener un efecto disruptivo en algunos de los sistemas con los que estamos familiarizados a todos los niveles. Como hemos dicho, en primer lugar, se implementó en el sector financiero con la introducción de Bitcoin, y más tarde se fueron desarrollando distintas versiones de Blockchain para suplir distintas carencias en distintos ámbitos de nuestra vida, no sólo en el ámbito financiero. A medida que esta nueva tecnología vaya siendo adoptada y conocida, cada vez serán más los usos que se le den. En cualquier caso, hoy por hoy tenemos ya un gran número de casos y ejemplos de la aplicación del Blockchain, y podemos dividir sus usos en dos grandes ramas principales: Aplicaciones financieras y aplicaciones no financieras.

2.6.1. Aplicaciones financieras

En general, en cualquier operación financiera hay una tercera parte que hace de guía entre personas u organizaciones. Estas terceras partes llevan a cabo las siguientes funciones (Mainelli, 2014):

1. Confirmar la autenticidad del intercambio
2. Evitar duplicaciones de la transacción financiera
3. Registrar y validar la operación
4. Hacer de agente en favor de clientes o asociados

La tecnología Blockchain consigue suplir las primeras tres propiedades arriba enumeradas. Ello permite al Blockchain ser utilizado en las siguientes aplicaciones financieras.

- *Criptomonedas*. Este es el caso más evidente de aplicación de la tecnología Blockchain, ya que es para el que fue concebida originalmente. Estos últimos años hemos podido comprobar como este ámbito ha ganado una enorme popularidad, y pese a que es visto por mucha gente como una burbuja con escaso recorrido, la realidad es que cuenta con los atributos necesarios como para revolucionar el sistema monetario actual, o como poco para convivir con él.

- *Acciones, derivados*. El mercado de acciones se rige por una autoridad central en cada país, como la CNMV en España. Estas autoridades centrales hacen un seguimiento de todas las transacciones y acuerdos a los que se llegan. Sin embargo, este proceso lleva asociados una serie de costes y no es ni mucho menos inmediato a la hora de realizar una transacción. Implementar el Blockchain en esta área reduciría los costes extra y los retrasos. En el caso de los derivados también puede tener un gran impacto, ya que mediante los Smart contracts desaparece la necesidad de una entidad reguladora. Las dos partes no tienen por qué confiar la una en la otra y no harían falta los famosos depósitos de garantía.

- *Seguros*. El Blockchain puede soportar las transacciones en los mercados de seguros entre los distintos clientes, compañías aseguradoras y los tenedores de pólizas. El Blockchain se puede utilizar para negociar, comprar y registrar pólizas,

presentar y procesar reclamaciones o llevar a cabo actividades de reaseguro entre las compañías. Muchas de las pólizas pueden automatizarse mediante el uso de Smart contracts, lo que reduciría enormemente los costes administrativos (Cohn et al, 2017).

- *Acuerdos financieros.* Las cadenas de bloques pueden utilizarse entre empresas y organizaciones para procesar, registrar y procesar acuerdos monetarios. Facilita los procesos de compensación que requieren ajustar las obligaciones de las partes para posibilitar los pagos. Los sistemas de negocio que estén basados en la tecnología Blockchain podrán integrase con otras aplicaciones basadas en Blockchain, como aplicaciones de comercio de acciones, o aplicaciones de logística para permitir que el intercambio financiero se lleve a cabo en la propia aplicación.

- *Transacciones financieras globales de usuario a usuario (P2P).* Hasta hoy, cualquier interacción financiera entre dos personas tenía que pasar por una entidad reguladora como garantía. Estas entidades necesitan verificar las transacciones y asegurarse de que se realizan de forma correcta. Sin embargo, muchas de esas transacciones pueden ya verificarse mediante el Blockchain. Como resultado se elimina al intermediario del proceso y los usuarios pueden verificar y asegurarse colectivamente de la correcta ejecución de estas transacciones. El beneficio adicional es que estas transacciones globales no tienen restricción alguna por parte de las entidades implicadas y las divisas utilizadas.

2.6.2. Aplicaciones no financieras

2.6.2.1. Sanidad

Una de las áreas más sensibles dentro de la industria sanitaria es el almacenamiento y gestión de los datos e informes de los pacientes, ya que son altamente confidenciales. El historial médico de los pacientes normalmente se distribuye entre varios sistemas manejados y poseídos por uno o varios proveedores sanitarios. Los avances tecnológicos de la última década han permitido la digitalización de los historiales médicos, creando lo que se conoce como Expedientes Clínicos Electrónicos. Sin

embargo, el compartir estos historiales entre los distintos proveedores sanitarios es algo bastante complejo y delicado, dada la sensibilidad de la información y las ataduras legales en cuanto a seguridad y privacidad. Es aquí donde el Blockchain puede utilizarse para garantizar la correcta y segura difusión de los historiales médicos entre los distintos hospitales y proveedores (Prisco, 2016).

2.6.2.2. Gobiernos y sector público

Aplicar el Blockchain al sector público tiene el potencial de agilizar enormemente un gran número de procesos burocráticos que son lentos y costosos simplemente por que requieren de la intermediación de la autoridad de turno. Además, al existir un gran número de autoridades competentes, la cooperación entre estas es también lenta y poco eficaz en muchas ocasiones. Implementar el Blockchain asegura la privacidad de los documentos, y certifica su autenticidad, eliminando en muchos casos estos procesos burocráticos (Crosby et al, 2016). Otra área gubernamental donde puede aplicarse esta tecnología es a la hora de votar. Hoy en día el sistema es bastante rudimentario si lo comparamos con otros aspectos de nuestra vida, y en aquellos países donde existe la opción de votar electrónicamente ha habido casos de fallos de seguridad y manipulación de resultados. Con el Blockchain puede crearse un sistema 100% seguro y sin fallos de seguridad, imposibilitando la posibilidad de votar dos veces, errores de conteo y suplantación de identidad.

2.6.2.3. Logística y manufactura

Las plataformas de gestión de logística utilizadas hoy día son softwares que ayudan a las empresas en la entrega de diversos productos, servicios o materias primas entre productores/vendedores y clientes. Estas plataformas normalmente están centralizadas y son propiedad de la propia empresa o se utilizan entre unas pocas empresas asociadas. El Blockchain puede llevar a estas plataformas a un nivel superior. Uno de los mayores retos en las plataformas de gestión de logística es la involucración de varias empresas en la actividad. Las cadenas de bloques pueden solucionar este problema y dotar a las plataformas de una flexibilidad que permita adaptarlas a la perfección a las necesidades de las empresas, pudiendo incluir sub-actividades sincronizadas y llevadas a cabo por distintas compañías dentro de la misma red, como

fábricas, empresas de almacenamiento, empresas de transporte y autoridades reguladoras (Al-Jaroodi, 2019). Usar un DL en Blockchain para verificar, almacenar y auditar las transacciones logísticas ayudará a reducir los retrasos en las entregas, los costes de gestión y los errores humanos. Además, aplicar los Smart contracts falicitará que los acuerdos y la cooperación entre las empresas involucradas y permitirá crear contratos entre ellas más rápido y con menos costes (Al-Jaroodi, 2019).

2.6.2.4. Energía

Este es quizá uno de los sectores donde más rápido se esta implementando la tecnología Blockchain, y donde podemos ver de forma palpable que la aplicación del Blockchain en la industria es algo real y que ofrece soluciones muy interesantes. Una de las razones de que este sector en concreto esté experimentando la implementación del Blockchain a una velocidad tan alta es precisamente porque es una de las áreas donde más regulación existe. El uso principal del Blockchain en el sector energético es con las micro redes energéticas. Una micro red es in foco localizado de fuentes de energía independientes integrados y gestionados con el objetivo de optimizar la producción de energía y la eficiencia de su consumo (Lasseter et al, 2004). Las fuentes de energía pueden ser generadores, instalaciones de energías renovables y estaciones de almacenamiento de energía propiedad de varias organizaciones, empresas o proveedores de energía. La principal ventaja de estas micro redes es que no sólo permite que los residentes y otros consumidores tengan acceso a la energía que necesiten, si no que también puedan producir y vender el exceso de energía que tengan a la red. En este aspecto el Blockchain puede utilizarse para facilitar, registrar y validar las transacciones de compraventa de energía en las micro redes (Cohn et al, 2017). Una empresa muy interesante que está implementando este proceso en Australia es Powerledger.

2.7. Limitaciones y retos del Blockchain

A pesar de las muy interesantes potenciales aplicaciones que pueda tener en Blockchain, uno de los factores más importantes en su desarrollo es saber donde está el límite, pues la tecnología Blockchain tampoco es apta para aplicarla en todo. No todos los procesos necesitan un sistema de pagos, una plataforma donde se puedan intercambiar valores o activos peer-to-peer, descentralización o una basta herramienta pública para

registrar y almacenar datos (Swan, 2015). También debemos tener en cuenta que la tecnología Blockchain se encuentra en un estado muy temprano de desarrollo y debe superar una serie de obstáculos antes de ser ampliamente adoptada (Bybit learn, 2022).

Las limitaciones actuales de las cadenas de bloques pueden explicarse con el llamado "trilema del Blockchain". Las cadenas de bloques cuentan con tres características fundamentales: Escalabilidad, seguridad y descentralización. Sin embargo, hoy por hoy no es posible crear una red escalable y segura sin que esta no sea descentralizada. Tampoco puede crearse una red descentralizada y segura y que además sea escalable, ni tampoco una red escalable y descentralizada y que además sea segura. Esto es lo que recibe el nombre de trilema del Blockchain, la incapacidad de aunar las tres cualidades en una misma cadena (Caballero et al, 2020). Uno de los elementos centrales de las cadenas de bloques públicas es dar la capacidad a cualquier nodo de unirse a la red y operar en ella. Cada nodo procesa cada una de las transacciones, y por tanto guarda una copia del historial de las transacciones de la cadena en su ordenador. Esto hace que las Blockchain sean tan fuertes como su eslabón más débil, ya que la escalabilidad y por lo tanto la velocidad de la red depende del nodo más débil (Blockchaines, s.f.).

Los principales retos que afloran cuando hablamos de Blockchains públicas son los siguientes:

2.7.1. Rendimiento

Cuando una transacción es procesada, una Blockchain debe realizar las mismas operaciones que una base de datos ordinaria, aunque con tres procesos adicionales (Song et al, 2016):

1. Verificación de la firma. Toda transacción de una cadena de bloques debe ser digitalmente firmada utilizando la clave privada. La generación y procesamiento de estas firmas son complejas desde un punto de vista computacional. Por el contrario, en bases de datos descentralizadas, una vez que se ha establecido una conexión no hay necesidad de verificar cada operación que entra.

2. Mecanismos de consenso. Ya hemos hablado sobre los distintos protocolos de consenso que existen y vimos como todos requerían en mayor o menor medida un esfuerzo computacional por parte de los nodos para llegar a ese consenso. En el proceso de llegar a ese consenso, los nodos deben lidiar con continuas anulaciones de transacciones y demás impedimentos. Una base de datos centralizada también se enfrenta a transacciones problemáticas y anuladas, pero a un nivel muy inferior.

3. Redundancia. Esto hace referencia al esfuerzo computacional realizado por la red en total para procesar una transacción. Mientras que en una base de datos normal procesa las transacciones una o dos veces, en una Blockchain todos los nodos de la red deben procesar cada transacción de manera independiente, con el consiguiente esfuerzo computacional que conlleva.

Teniendo todo esto en cuenta, deducimos que la limitación de rendimiento del Blockchain proviene de mudar de un sistema centralizado a uno descentralizado. El tener un sistema descentralizado conlleva incorporar mecanismos más complejos a la hora de procesar las transacciones, como los tres mencionados arriba. En consecuencia, el tiempo que se dedica a procesar una transacción en una Blockchain es significativamente superior al tiempo requerido en una base de datos central.

2.7.2. Escalabilidad

En las Blockchain públicas la escalabilidad es el mayor de los retos a los que se enfrentan. El mayor obstáculo para lograr esa ansiada escalabilidad es que cuanto más crezca una cadena, mayores serán los requisitos de almacenamiento, ancho de banda y esfuerzo computacional que deben invertir los nodos de la red. Existe la amenaza de que ante un incremento de la capacidad técnica de los nodos, cada vez sean menos los capaces de procesar los bloques, y ello lleve a una mayor centralización dentro de la propia cadena (James-Lubin, 2015).

2.7.3. Consumo de energía

En un mundo en el que cada vez más se mira con lupa el impacto ecológico de las compañías y nuevas tecnologías, el Blockchain entra en contraste por el gran consumo de

energía que conlleva su principal mecanismo de consenso, el Proof of Work. Si bien es cierto que hay otros protocolos de consenso que consumen mucha menos energía, el PoW sigue siendo el más utilizado y el que más garantías ofrece de seguridad. Será interesante observar cómo logra Ethereum (la segunda Blockchain más importante tras Bitcoin) sustituir el PoW por el PoS y hasta qué punto puede este suplir de manera efectiva el PoW.

Actualmente la tecnología Blockchain se encuentra sumida en un estado de ebullición en el que cada día surgen nuevos proyectos buscando solucionar estos tres retos. En concreto existen dos nuevas formas de DL que han cobrado cierta relevancia por la posible viabilidad de sus proyectos. Estos son DAG (Directed Acyclic Graph) y Hashgraph. Son dos nuevos conceptos de red descentralizada que difieren del Blockchain en la estructura de la cadena, solucionando a priori los problemas de escalabilidad. El concepto de DAG más avanzado lo representa IOTA, que tiene su propia Blockchain, y el proyecto Hashgraph está patentado por Hedera.

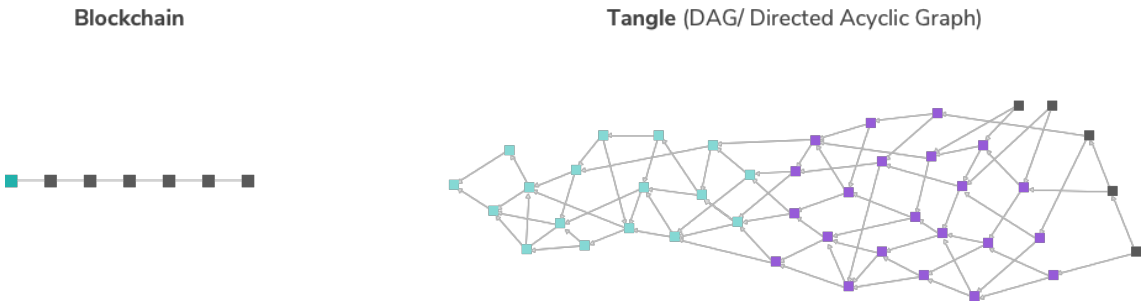

Imagen 8: Comparativa de una cadena Blockchain y DAG (Blockchaines, s.f.)

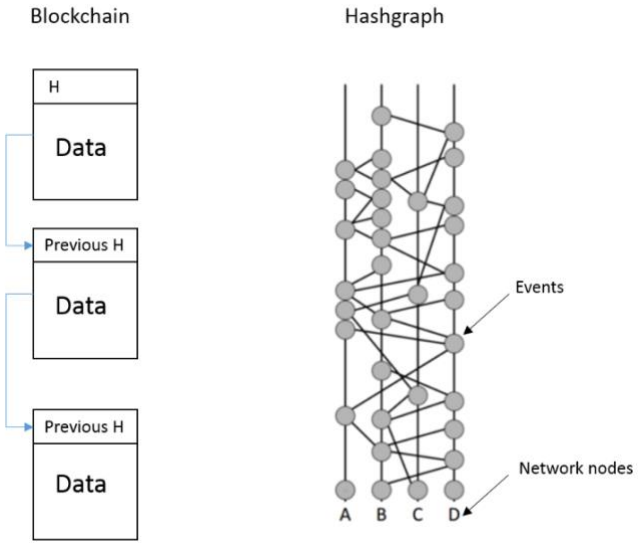

Imagen 9: Comparativa de una Blockchain y Hashgraph (Blockchaines, s.f.)

Aunque estos dos proyectos no son más que dos "embriones" y aún tienen que demostrar si de verdad son viables y pueden suplir las carencias del Blockchain como dicen, no deja de ser interesante el nivel de innovación en el sector y las nuevas ideas que surgen.

2.8. Casos relevantes

Un caso interesante y relevante de aplicación real de la tecnología Blockchain a la gestión de la identidad digital es el caso de Estonia, con la red KSI Blockchain.

La tecnología blockchain no es algo nuevo para Estonia, pues desde 2012 se viene implementando para proteger datos nacionales, prestar servicios electrónicos y proteger dispositivos inteligentes tanto en el sector público como privado. Estonia utiliza esta tecnología para reforzar la integridad de los datos gubernamentales y sus sistemas. La Autoridad de Estonia de Sistemas de Información (RIA) es un proveedor de servicios integral del gobierno, que garantiza el acceso a la red Blockchain de las autoridades estatales a través de la infraestructura X-road (e-estonia, 2020).

Algunos de los registros públicos soportados por la red Blockchain son el registro de sanidad, el registro de propiedad, el de empresas, el sistema de tribunales digital, los servicios información de vigilancia o los anuncios oficiales del estado (e-estonia, 2020). En el caso de Estonia, el proveedor de su red KSI Blockchain es la empresa Guardtime, que les presta el servicio de dicha red, diseñada explícitamente para el estado de Estonia. Como ya sabemos, las redes Blockchain consisten en un DL en el que todos los integrantes de la red pueden ver los datos y transacciones en el contenidos, sin embargo, en este caso Guardtime va más allá, y también publica periódicamente los datos de la red en periódicos como Financial Times. Esto implica que ante una hipotética manipulación de los registros, el atacante no sólo tendría que manipular la red en sí, si no también alterar miles de copias de periódicos ya publicadas, haciendo la estafa del todo imposible, ya que ni la propia empresa proveedora tiene capacidad para hacer tal cosa. Como resultado, mientras que en un proveedor central de datos gubernamental lleva normalmente unos 7

meses en localizar una brecha en el sistema, en una red Blockchain puede localizarse en cuestión de minutos (e-estonia, 2020).

Es importante aclarar que la empresa proveedora de la tecnología en ningún momento tiene acceso a los datos contenidos en la red, si no que simplemente proporciona la plataforma de tecnología Blockchain que permite asegurar la integridad y seguridad de los datos. En el caso de que la compañía proveedora desapareciese, esto no afectaría a la información contenida en la cadena, pues esta seguiría siendo verificable por todos los nodos de la red que contienen una copia del DL, además de que la información se publica en los periódicos.

Es especialmente relevante en este trabajo la aplicación de esta tecnología en la identidad digital por parte del estado estonio. Todos los estonios, sin importar donde vivan, tienen una identidad digital emitida por el gobierno. Este sistema de identidad digital, llamado e-ID, es la piedra angular del sistema electrónico del país. El e-ID y todo el sistema que lo rodea es parte del día a día en las transacciones diarias de los ciudadanos, tanto en el sector privado como en el público. La gente utiliza sus e-ID para pagar facturas, comprar, votar online, firmar contratos, acceder a sus datos sanitarios y mucho más (e-estonia, 2020). Digo que es relevante porque este sistema lleva funcionando plenamente durante los últimos diez años y es un caso contrastado de éxito y eficiencia.

2.9. Conclusión

En esta primera parte del trabajo hemos estudiado cómo funciona la tecnología Blockchain, de qué elementos se compone, qué tipos hay, en cuantas categorías puede clasificarse y cuáles son sus principales hándicaps y retos.

Podemos concluir que el verdadero valor de la tecnología es su flexibilidad y capacidad de adaptación, pudiendo emplearse en los más diversos sectores y en todo tipo de empresas. Para mí, la utilidad real de las cadenas de bloques no es su uso como divisa, si no la capacidad de ciertas cadenas de implementarse a nivel privado (empresas que quieran agilizar sus procesos) y a nivel público (administraciones estatales, gestión de identidades digitales, digitalización de procesos, etc).

3. La identidad digital

Para comprender lo que es una identidad digital, primero debemos ahondar en el concepto más amplio y profundo de identidad como tal. Este es un debate filosófico que lleva presente en nuestra sociedad desde que existimos. En filosofía, el término identidad se refiere a la respuesta a la pregunta ¿Quién soy? La respuesta es el conjunto de cualidades y características únicas que hacen de cada uno de nosotros un individuo único y diferente del resto (Olson, 2016). De modo que la identidad hace referencia a todo el conjunto de cualidades y características que definen a una entidad y que sea distinguible y reconocible cuando es comparada con otras entidades (Ayed, 2014). De igual forma, una identidad digital es una identidad que permite identificar a un individuo o compañía en la red. Hoy, en un contexto en el que el internet de las cosas (IoT), está tan arraigado en nuestro día a día, y con una creciente dependencia de este, podemos afirmar que la identidad de un individuo se compone tanto de su identidad personal (nombre, apellidos, fecha de nacimiento, número de pasaporte o de la seguridad social…) como de su identidad digital. En el contexto digital, una identidad es un conjunto de archivos digitales que representan a un usuario. Estos archivos son guardados y gestionados en un formato estándar por las entidades que proveen la información de la identidad o los requisitos necesarios para completar una transacción. Una identidad digital acepta e integra nuevos archivos para crear una visión cada vez más completa y rica del usuario.

Al ser un concepto algo abstracto el de la identidad digital, hay una serie de definiciones al respecto:

El Sistema Global para las Comunicaciones Móviles estableció que, en el mundo actual, nuestras identidades digitales están convirtiéndose en parte de nuestras vidas a medida que mudamos a un mundo dominado por internet, y estas identidades permiten predecir como nos comportaremos y comerciaremos. Para el ámbito empresarial, aprovechar la identidad digital es y será un elemento crucial, sobre todo a la hora de cumplir ciertos requerimientos de CDD (customer due diligence) (Kvitnitsky, 2018).

Por otra parte, la Organización Europea para la e-identity y la seguridad, EEMA, enfatiza en que la identidad digital lleva bastante tiempo existiendo entre nosotros, sólo que es complicado ligar una persona física a una identidad digital que les permita acceder

a su cuenta de correo, bancaria, de dinero digital y en definitiva a una nueva era de transformación digital de una forma segura y eficiente (Erik, 2018).

En un estudio realizado por Secure Identity Alliance, estos enfatizan en el uso eficiente y efectivo de los métodos de identidad tradicionales tales como certificados de nacimiento combinados con la utilización de la tecnología para permitir y asegurar métodos de identidad digital, que puede llevarse directamente en la forma de una tarjeta inteligente o en un smartphone (Secure identity Alliance, 2018).

La identidad de las personas es intrínseca al correcto funcionamiento de la sociedad y la economía, y el poder contar con una forma eficiente de identificarnos a nosotros mismos y nuestras posesiones nos permite crear sociedades dinámicas y mercados globales (Consensys, s.f.). Como se menciona en el párrafo anterior, en su nivel más básico la identidad se compone de una serie de atributos personales (nombre, apellidos, fecha de nacimiento, número de pasaporte o de la seguridad social…) que son emitidos por organismos centrales (gobiernos) y se almacenan en bases de datos centralizadas (Consensys, s.f.). El hecho de que una información tan sensible se almacene concentrada en unos servidores centrales presenta ya de por sí un riesgo significativo, sobre todo en una época en la que los hackeos masivos a gobiernos están a la orden del día. Además, no solo debemos tener en cuenta el riesgo de hackeo por parte de terceros, si no el posible mal uso de esos datos por personas o instituciones con acceso a esos servidores.

En la actualidad ya no es posible confiar completamente en los métodos de identidad tradicionales, además de que la sociedad espera métodos de identificación que permitan una mayor agilidad, seguridad y una conectividad permanente.

Existen tres partes relevantes en el contexto de la manipulación de la identidad, ya sea digital o personal. En primer lugar, las propias personas, dueñas de su identidad. En segundo lugar, las empresas, que cada vez juegan un papel más importante en la gestión de nuestra identidad digital generada en internet. Y por último los gobiernos, que como hemos dicho, generan y almacenan nuestros datos personales. Como en cada uno de los tres casos anteriores la información se gestiona y almacena de manera individual y centralizada (gobiernos por una parte, empresas por otra y nosotros mismos por otra),

surge una fragmentación en la integridad de nuestra identidad y el riesgo de que esta no sea gestionada de forma adecuada es aún mayor, sobre todo porque escapa a nuestro control la gestión que estas instituciones ejercen sobre nuestros datos. Uno de los casos más relevantes en cuanto a este problema es el de Facebook, empresa que se vio envuelta en un proceso judicial con tal de esclarecer que se hacía con los datos de los usuarios, cosa que a día de hoy no se ha esclarecido.

3.1. El surgimiento de la identidad digital

Una identidad defina la singularidad de un individuo como un ente consistente cuando se compara a lo largo de un período de tiempo. Fearon define la identidad como la uniformidad de una persona u objeto en todo momento y circunstancia, la condición o hecho que hace que ese individuo sea el mismo y no otro (Fearon, 1999).

El propósito de la identidad digital es hacer de puente entre la identidad física de un individuo y las instituciones públicas y privadas. De media, un usuario de internet crea en torno a 150 cuentas distintas en internet, para comprar, consultar información o servicios. (WEF, 2018). Actualmente, un individuo puede ser identificado por sus atributos, metadatos y la información que este genera en internet, permitiendo la predicción de la actividad del individuo en internet, cosa que no era posible con la identificación física tradicional (OECD, 2015). Podemos deducir que la identidad digital es producto natural de nuestro comportamiento y hábitos en la red. Debido a la sensibilidad e importancia de los datos que generamos en internet, es vital dar con un sistema que nos permita tener un control sobre nuestra identidad digital, cosa que hoy por hoy no tenemos. De ahí el propósito de este estudio.

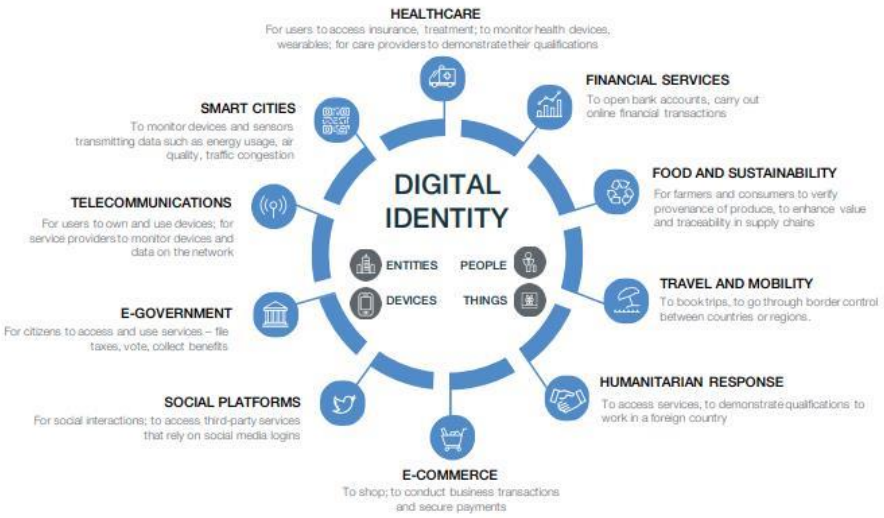

Imagen 10: La identidad digital en la actualidad (WEF, 2018)

3.2. Problemas actuales de la identidad digital

Por tanto, podemos identificar tres problemas principales que existen actualmente en lo relativo a la identidad de las personas: en primer lugar nuestra falta de control sobre nuestra propia información, en segundo lugar la falta de seguridad en los sistemas de almacenamiento actuales por parte de empresas y gobiernos, y por último la monetización y comercialización de nuestros datos.

Ya hemos explicado nuestra incapacidad para controlar cómo se gestiona nuestra información, pero aparte de esta falta de control de los individuos sobre su identidad, existe otra variante del problema. Aún existen muchas regiones del mundo donde un porcentaje muy significativo de la población no tiene ninguna forma de identificación, ni física ni digital. Se estima que en torno a 1000 millones de personas no tienen ningún tipo de identidad. Esto es una barrera enorme para el desarrollo de esos habitantes y por extensión del país, ya que sin una identificación física, esos individuos no tienen manera de acceder al sistema económico, puesto que no pueden acceder a la escuela, a una cuenta bancaria, trabajos… Sin embargo, muchas de esas personas sin identidad física sí que tienen acceso a un dispositivo inteligente, lo cual les permitiría contar con una identidad digital reconocida.

El segundo problema radica en que en los últimos veinte años se ha desarrollado de forma muy rápida todo lo relativo a los propios dispositivos inteligentes, mientras que el desarrollo de los servidores y sistemas que sustentan estos dispositivos no se ha producido al mismo ritmo, generando un desajuste. Hasta hace poco el tema de la seguridad ocupaba un segundo plano en el desarrollo tecnológico, y no ha sido hasta ahora cuando las empresas han comenzado a darle más importancia, debido a los hackeos a gran escala que ahora ocupan gran parte de las conferencias más importantes de seguridad digital. actualmente almacenamos nuestra información personal más valiosa en bases de datos centrales del gobierno, que se sustenta en sistemas de software con múltiples puntos débiles. Son estos servidores que contienen la información personal de millones de personas los objetivos más lucrativos para los piratas informáticos (Consensys, s.f.). Estos servidores están sujetos a continuos ataques informáticos, y se estima que el 97% de todas

las brechas de seguridad en 2018 ocurrieron en servidores conteniendo Información de Identificación Personal (PII) (Consensys, s.f.).

El tercer problema se encuentra en la comercialización de los datos. Los datos se han convertido en un activo valiosísimo, capaz de generar una riqueza enorme y permitiendo a las empresas ofrecer un mejor servicio a sus clientes. Sin embargo, este es un tema de una complejidad ética muy grande. Por una parte, existe una línea muy delgada entre una correcta utilización de los datos por parte de las empresas para prestar un mejor servicio y entre un uso poco ético, dejando de lado los intereses de los individuos que generan esos datos y primando los intereses de la compañía. Por otra parte, los usuarios tienen una identificación digital fragmentada, y sin saberlo pierden el valor que sus datos generan.

3.3. ¿Por qué es inevitable el cambio hacia una identidad digital?

Cada dos años, la Organización de las Naciones Unidas realiza un estudio en los 193 estados miembros acerca de los avances y desarrollos en el ámbito digital. El estudio de 2018 demostró que en los dos últimos años los trámites digitales online en distintas áreas habían incrementado de un 18% a un 47%, evidenciando la creciente participación de los individuos hacia una nueva transformación digital. En el estudio de 2020 se confirmó esta tendencia, aumentando hasta un 60% de media. Debemos tener en cuenta que en esa media se incluyen una gran cantidad de estados que se encuentran en un estado de desarrollo bastante, lo cual camufla el dato, pero no deja de evidenciar el crecimiento. También tenemos que tener en cuenta que en el estudio no se recoge el impacto del covid, cosa que ha acelerado enormemente la transición hacia la digitalización. Para bien o para mal, la pandemia ha evidenciado el enorme margen de mejora de las instituciones públicas y privadas en cuanto a la eficiencia de los trámites tradicionales se refiere. En muchos casos estos pueden ser sustituidos por trámites online infinitamente más rápidos y sencillos.

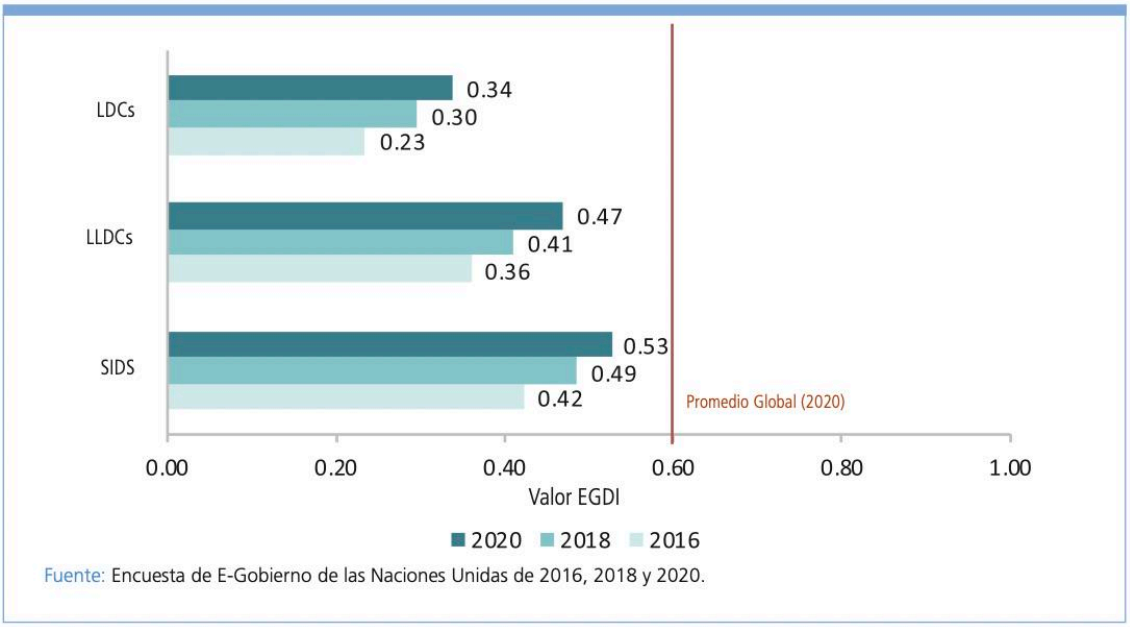

Imagen 11: Encuesta de e-gobierno de las UN (UN, 2020)

Para asentar de forma definitiva esta tendencia, se debe de hacer estas transacciones algo seguro y fiable, cosa que tan sólo puede conseguirse con una identidad digital robusta, uniforme y definida.

Servicios transaccionales disponibles en línea	2018	2020	Variación Porcentual
Solicitar acta de nacimiento	83	149	80
Solicitar permiso de construcción	55	136	147
Solicitar licencia comercial	103	151	47
Solicitar certificado de defunción	74	147	99
Solicitar licencia de conducir	59	144	144
Solicitar permisos ambientales	74	131	77
Solicitar vacantes gubernamentales en línea	132	156	18
Solicitar el registro del título de propiedad	67	132	97
Solicitar certificado de matrimonio	78	146	87
Solicitar tarjeta de identificación personal	59	135	129
Solicitar programas de protección social	85	112	32
Solicitar visa	99	95	-4
Declarar a la policía	84	90	7
Pagar multas	111	115	4
Pagar los servicios públicos (agua, gas, electricidad)	140	145	4
Registrar una empresa	125	162	30
Registrar un vehículo con motor	76	82	8
Presentar cambio de dirección	58	66	14
Presentar impuestos sobre la renta	139	143	3
Presentar impuesto al valor agregado	116	130	12

Imagen 12: Tendencia de los servicios transaccionales en línea 2018-2020 (UN, 2020)

En la tabla superior comprobamos una vez más la clara tendencia al alza de los trámites en línea. En ella se muestra el número de países que ofrece la posibilidad de realizar cada trámite online, y la variación porcentual respecto a 2018.

Además, como ya hemos mencionado en el estudio, actualmente existen aproximadamente 1.100 millones de personas sin ningún tipo de identificación que acredite su identidad, siendo la identidad digital una potencial solución a este problema, como también señala la UN en su estudio.

3.4. Sistemas de gestión de la identidad digital

El mundo digital avanza constantemente, proveyendo a los usuarios de nuevas formas de comunicación, nuevos servicios, nuevas formas de negocio… Y a medida que avanzan las nuevas tecnologías avanzan también los sistemas de gestión de los datos generados por los usuarios. Cada vez se genera más información, de mejor calidad, más estratificada y por consiguiente de un mayor valor económico, aunque esto conlleva a que también es de una mayor sensibilidad. La cantidad de información sensible controlada por terceras partes con poco o ningún control de los usuarios ha incrementado exponencialmente en los últimos años (Pimenidis, 2010).

Por ello, la gestión de la identidad ha surgido como una nueva práctica vital en las organizaciones de hoy. Al ser un término relativamente nuevo, no existe una definición exacta y globalmente aceptada que lo identifique, pero sí se coincide en que la gestión de la identidad es el proceso organizacional para identificar, autenticar y autorizar a individuos o grupos de individuos el acceso a aplicaciones, sistemas o redes mediante la asociación de los derechos de esos individuos con identidades establecidas (Rouse, 2017).

Al fin y al cabo, la gestión de la identidad trata de establecer una relación entre individuos en el mundo físico para brindar servicios o acceder a información en el mundo digital con confianza y confiabilidad.

Desde la concepción de internet han aflorado diversos sistemas y técnicas de gestión de la identidad, siendo los principales utilizados hasta ahora el Isolated Identity

Management Model, el Centralized Identity Management y el sistema Federated Identity Management.

Isolated Identity Management Model:

En adelante nos referiremos a este sistema como IIMM. En este sistema el proveedor del servicio juega un papel crucial como proveedor de la identidad que conduce al almacenamiento de las operaciones del usuario en un solo servidor. En este modelo, la autenticación, asignación y autorización de una identidad digital está facultada por un solo proveedor de servicios que actúa como atributo, identificador y proveedor de autenticación (Yuan Cao, 2010).

Este modelo se basa enteramente en la memoria del usuario, por lo que este debe mantener la identidad correspondiente a cada servicio.

Al ser uno de los sistemas más básicos y viejos, es más propenso a tener fallos de seguridad. Sin embargo, al ser independiente y contar con una identidad diferente para cada servicio, el fallo en la seguridad de uno de ellos no implica ningún riesgo para el resto de los proveedores. A medida que evoluciona internet este sistema se vuelve más inapropiado e ineficiente, ya que los usuarios tienen que acordarse de cada vez más credenciales, y el olvido de cualquier contraseña implica gastar bastante tiempo en recuperarla.

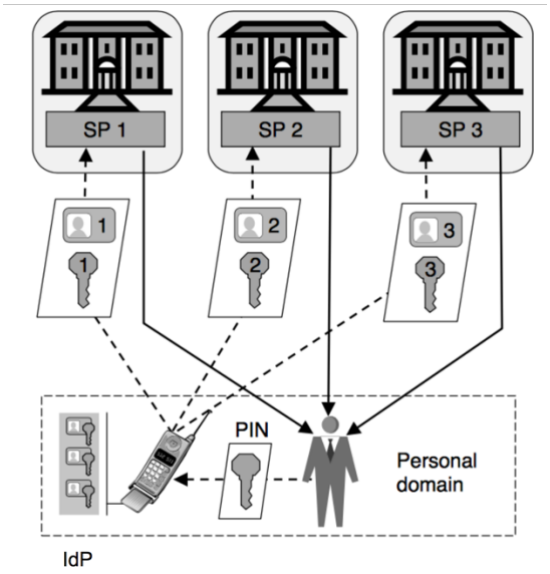

Imagen 13: Modelo de un Sistema IIMM (Josang et al, 2017)

Centralized Identity Mangement:

Este sistema difiere del IIMM en que en este sistema se implementa una solución Single Sign-on (SSO), lo cual permite que un usuario acceda a múltiples servicios sin tener que iniciar sesión con múltiples cuentas. Esto requiere una relación de confianza entre usuario, proveedor y entidades asociadas. Este sistema reduce la frustración del usuario y la fatiga de contraseñas a la vez que se incrementa la seguridad (Griffith, 2021).

En general, este sistema se externaliza a un proveedor de identidad central que se dedica exclusivamente a gestionar los servicios de identificación, credenciales y el ciclo general de la identidad de los usuarios. La información de los usuarios se almacena en un repositorio central del proveedor de la identidad (Bernd Zwattendorfer, 2014). La contrapartida de este sistema es que cualquier fallo técnico en el proveedor lleva a la inaccesibilidad de cualquier servicio ligado a ese proveedor (Ajhoun, 2014). Curiosamente, la principal ventaja de este sistema frente al IIMM, es también su principal desventaja. Mientras que en el IIMM el fallo en la seguridad de una cuenta no implica riesgo alguno para el resto, en este caso si hay algún tipo de ataque en la base de datos del proveedor de la identidad, toda la información de todas las cuentas de los usuarios se habrá visto comprometida. Así mismo, cuantos más usuarios maneje el proveedor, más ineficiente y peor funcionará el sistema (Yuan Cao, 2010).

Federated Identity Mangement:

Este sistema es el más avanzado de los utilizados actualmente por las organizaciones para gestionar las identidades digitales. El sistema de identidad federal se basa en un grupo de organizaciones que tienen un acuerdo común cimentado en una relación de confianza para intercambiar información.

El FIM puede definirse como una serie de estándares y tecnologías comunes que permiten a una serie de proveedores de servicios autenticar las identidades de otro proveedor miembro del sistema FIM (Yuan Cao, 2010). Esta aproximación ayuda a reducir el número de identidades de cada usuario, pero tiene ciertas limitaciones tales

como identificar a los proveedores de identidad y la continua amenaza al robo de las identidades. Una brecha en el sistema de seguridad otorga al hacker acceso a la información de todos los integrantes de la FIM (Ajhoun, 2014).

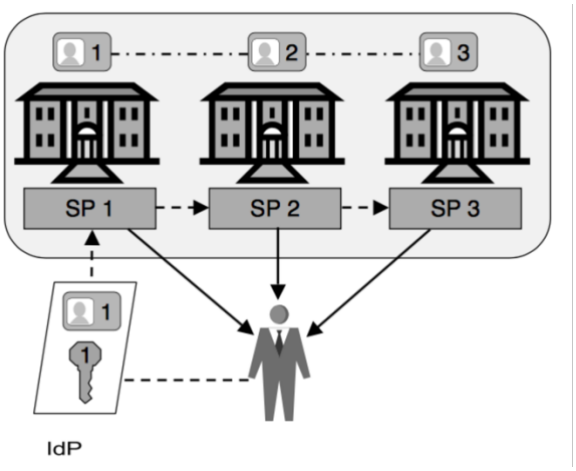

Imagen 14: Modelo de un Sistema FIM (Josang et al, 2017)

3.5. Conclusiones sobre los sistemas de gestión de la identidad actuales

Si ponemos en común los tres sistemas vistos, podemos ver que todos tienen en común un problema, que es la vulnerabilidad a los ataques informáticos. En el momento en que un hacker consigue acceder a la base central del proveedor, toda la información de los usuarios queda al descubierto. En el sistema IIMM esto no ocurre porque el usuario tiene una clave para cada proveedor de servicios, sin embargo, esto es tremendamente ineficiente y cada vez menos práctico. Por tanto, en líneas generales vemos que hasta la fecha no se ha implementado ningún sistema que aúne seguridad y escalabilidad.

4. Blockchain en la Identidad Digital

La identidad digital es básica en un mundo como el nuestro, tanto para las personas como para las empresas y gobiernos puesto que cada vez se utiliza para más transacciones, más negocios y para acciones cotidianas. Sin embargo, como hemos visto los sistemas convencionales de gestión de la identidad son costosos y ralentizan el desarrollo y la mejora de las experiencias de los usuarios en internet. La introducción del Blockchain en este ámbito introduce una nueva forma de gestionar la identidad de las personas y las entidades. En este capítulo estudiaremos qué atributos de la tecnología Blockchain son los que permiten que se aplique de manera exitosa en el ámbito de la identidad.

4.1. Self-Sovereign Identity Management

Con las cadenas de bloques los usuarios tienen la capacidad de crear su propia identidad y registrarla en la cadena, ganando el control completo sobre ella y almacenándola de forma segura. Mediante el uso de esta tecnología los usuarios tienen control sobre quién puede acceder a su información personal.

El sistema mediante el cual se introduce el Blockchain en la gestión de la identidad recibe el nombre de Self-Sovereign Identity. El sistema SSI se considera como el último paso en la evolución de los sistemas de gestión de identidad de la era de IoT. Provee una combinación de seguridad, control individual y portabilidad que permite a los individuos y organizaciones controlar por completo y ser dueños absolutos de su identidad digital. El individuo por sí mismo es el proveedor de su propia identidad sin la necesidad de una tercera parte (Tobin, 2017). Existen 10 atributos principales que permiten al usuario controlar su identidad digital en un sistema SSI (Allen, 2016):

1. Existencia – la identidad digital siempre debe ir ligada a un ente físico. No puede existir una identidad digital que sea completamente virtual y no represente a ningún ente físico. La identidad digital debe servir de nexo entre la realidad y lo virtual.

2. Control – el usuario siempre debe tener el control completo de su identidad.

3. Transparencia – los sistemas SSI deben ser transparentes, por ello es vital el Blockchain. Deben ser sistemas abiertos tanto en su funcionamiento como en su gestión.

4. Accesibilidad – los usuarios deben tener total acceso a su identidad sin restricciones.

5. Portabilidad – la identidad digital debe poder ser portable, por ejemplo en forma de un código QR o una tarjeta digital.

6. Perseverancia – La identidad digital debe perseverar en el tiempo igual que lo haría una identidad física. Esta identidad debe durar tanto como el dueño de la identidad quiera. Habrá elementos de la identidad que requieran renovarse como la clave privada, y la identidad en sí estará sujeta a cambios en el tiempo, enriqueciéndose y siendo cada vez más completa.

7. Versatilidad – la identidad digital debe ser tan versátil como se pueda, sirviendo para tantas tareas y transacciones como sea posible. La idea general de la identidad digital es la de sustituir la gran cantidad de identidades digitales que tenemos actualmente por una sola, segura y transparente.

8. Consentimiento – los usuarios deben consentir el uso de su información por parte de empresas e instituciones.

9. Minimización – la información del usuario revelada en cada trámite debe ser la mínima necesaria. Por ejemplo, si una institución o empresa requiere saber la edad de un individuo, la información revelada debería ser los años que tiene, pero no la fecha de nacimiento.

10. Protección – los derechos de los usuarios deben ser protegidos en todo momento. En un caso de conflicto de intereses entre los derechos de una institución y los de un individuo, deben prevalecer los del individuo.

Aparte de estas 10 propiedades principales mencionadas por Allen existen otras tres propiedades del Blockchain que lo hacen apto para ser usado en la identidad digital: Costes de transacción bajos, inmutabilidad y comodidad.

Bajos costes de transacción: Las cadenas de bloques eliminan a los intermediarios, por lo que los costes de transacciones son más bajos.

Inmutabilidad: Las cadenas de bloques al ser completamente transparentes (toda la información queda registrada en la cadena y cualquier usuario puede consultarla en cada momento) eliminan cualquier riesgo de creación de identidades fraudulentas.

Comodidad: Los usuarios pueden realizar las transacciones desde cualquier lugar y desde cualquier dispositivo.

Las cadenas Blockchain tienen la capacidad de ser utilizadas en el ámbito de la identidad digital como medio de almacenamiento y transmisión de información. La tecnología DLT puede ser utilizada como medio descentralizado, otorgando a los usuarios la capacidad de almacenar su información de forma segura y transparente en la cadena, a la vez que es salvaguardada su privacidad (WEF, 2016). Recordemos que en una cadena de bloques toda la información en ella contenida está disponible para cualquier usuario, sin embargo, la información es anónima y es imposible saber a quién corresponde. De esta forma se aúna transparencia y privacidad en el mismo sistema.

4.2. Mecanismo Handshake

Como hemos visto la tecnología Blockchain hace uso de la criptografía para garantizar la solidez de la cadena. El proceso crítico que sustenta el mecanismo de autenticación recibe el nombre de mecanismo handshake (Dittmar, 2016). Este mecanismo elimina la necesidad de utilizar a una tercera parte para autenticar transacciones al establecer una interacción directa entre usuario y proveedor. El

proveedor de un servicio puede ser por ejemplo una página web, una institución pública, una tienda online… El mecanismo puede dividirse en tres pasos:

1. **Inicio de sesión** – En este primer paso, en lugar de utilizarse un nombre de usuario y una contraseña, el proveedor del servicio utiliza un código QR como método de autenticación. El próximo paso consiste en verificar la solicitud de inicio de sesión y crear una respuesta.

2. **Verificar la solicitud** – En este segundo paso se lleva a cabo el procedimiento para determinar si la solicitud de inicio es válida. Primero, se utiliza la clave pública para verificar que los datos de la solicitud de inicio son legítimos. Esto permite al proveedor firmar la solicitud, que entonces es publicada en la cadena. A continuación, se crea una app-identity en la blockchain. Es entonces cuando el usuario pulsa la opción de "verificar inicio de sesión".

3. **Elaborar una respuesta** – El último paso del proceso es crear una respuesta cuando el usuario hace click en el botón de "verificar inicio de sesión". Tras esto, la app (proveedor) crea una respuesta, la firma, y la manda de vuelta al usuario. Esta respuesta es verificada mediante el uso de un PKI (public key infraestructure) en la app y el usuario inicia sesión.

4.3. Sistemas de gestión de identidad basados en Blockchain

A pesar de ser una tecnología en un estado temprano de desarrollo y que aún no se ha aplicado masivamente a la gestión de la identidad, sí que hay una serie de proyectos en funcionamiento. Vamos a repasar los principales:

- **Sovrin**. Sovrin se ha diseñado específicamente para el uso de credenciales digitales. Sovrin implementa una SSI que no depende de ninguna autoridad central y que perdura en el tiempo. Los principales atributos de Sovrin son la gobernanza, escalabilidad y accesibilidad. Sovrin es una Blockchain pública que se basa en Hyperledger. Sovrin utiliza el protocolo de consenso zero-knowledge para

garantizar la privacidad de los usuarios (Tobin, 2016). Sovrin fue la primera SSI en utilizarse, y está enfocada al sector privado. Actualmente está mudando a una cadena que permita la adopción de Sovrin por otros sectores e industrias de manera más sencilla.

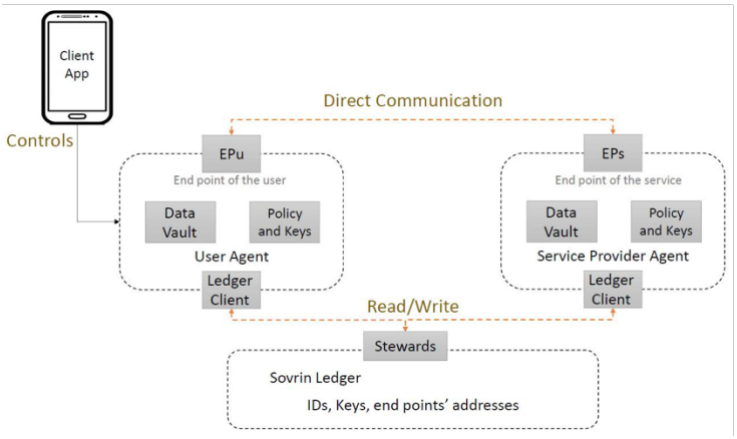

Imagen 15: Arquitectura de Sovrin (Alsayed et al, 2019)

- **uPort**. A diferencia de Sovrin, uPort es una cadena privada que depende de Ethereum. uPort se compone de tres elementos para funcionar: Smart contracts, bibliotecas de desarrolladores y una app móvil. La clave del usuario se guarda en la app, y los Smart contracts de Ethereum son la herramienta que permite a los usuarios recuperar su clave en caso de que pierdan el dispositivo móvil. Por último, las bibiotecas de desarrolladores permiten a otros desarrolladores y proveedores de servicios integrar uPort en sus propias apps. uPort table es el Smart contract utilizado por todas las identidades que utilizan uPort, y es la base para la autenticación y la transferencia de información sin necesidad de conexión a internet (Lundkvist et al, 2017).

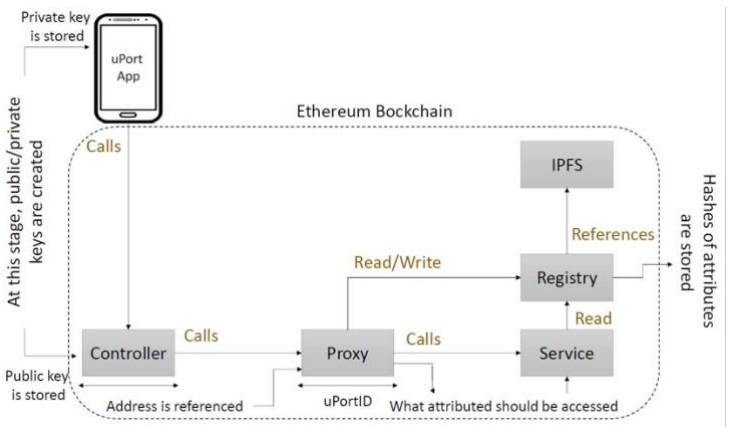

Imagen 16: Arquitectura de uPort (Alsayed et al, 2019)

- **ShoCard**. Este sistema SSI permite a los usuarios almacenar y proteger en la cadena su identidad digital. La información de la identidad digital del usuario siempre va ligada a la clave privada de este para asegurar la privacidad. Esto elimina la necesidad de usar una base de datos gestionada por un tercero. ShoCard mantiene el código de autenticación de la información del usuario en la blockchain, que garantiza la legitimidad de la identidad del usuario y facilita la verificación de esta. ShoCard también cuenta con su propio Token para realizar transacciones en la cadena, que es pública.

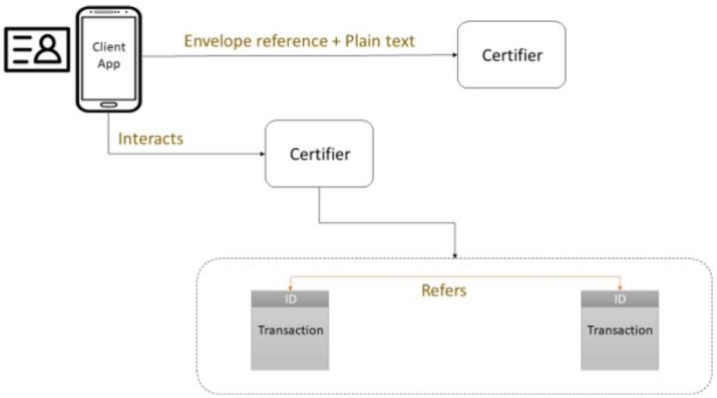

Imagen 17: Arquitectura de ShoCard (Alsayed et al, 2019)

5. Comparación de los distintos sistemas de Identidad digital basados en Blockchain

Para comparar los distintos sistemas SSI nos hemos basado en los principios de Allen para la Self-Sovereign Identity (Allen, 2016).

Principios del Self-Sovereign Identity	Sovrin	uPort	ShoCard
Existencia	9	9	9
Control	9	9	9
Acceso	9	9	9
Transparencia	9	9	9
Perseverancia	9	9	9
Portabilidad	9	6	9
Versatilidad	9	9	6
Consentimiento	9	6	9
Minimización	6	6	6
Protección	9	3	6
TOTAL	87	75	81

Comparación de los tres sistemas estudiados de SSI (elaboración propia)

Criterio de puntuación:

· 0 – No incluido en el planteamiento del sistema
· 3 – No mencionado en el planteamiento, pero se presupone incluido
· 6 – Incluido en el planteamiento, pero incompleto
· 9 – Incluido en el planteamiento de forma completa y concisa

Vemos que las tres soluciones cumplen en mayor o menor medida los principios expuestos por Allen para lograr una SSI óptima. De los tres, el más completo es Sovrin, teniendo mucho que ver que es el primer sistema planteado y el más avanzado y el que más se ha implementado de forma real en el mundo. ShoCard y uPort son soluciones algo

más flexibles que Sovrin, aunque con elementos con cierto margen de mejora, sobre todo en el ámbito de la protección del usuario. En el caso de Sovrin siempre prima el interés del usuario mediante el uso de algoritmos independientes que funcionan de manera descentralizada. En los otros dos sistemas los algoritmos no están tan avanzados y no han sido diseñados específicamente con ese objetivo.

La propia naturaleza de las cadenas de bloques permite eliminar el problema del almacenamiento centralizado de la información, cambiándolo por un almacenamiento descentralizado, repartido por los nodos que componen la red. Además del almacenamiento descentralizado, el Blockchain proporciona otras ventajas como una mejor eficiencia y una seguridad mucho superior (Mikula et al, 2018).

6. Conclusiones

Vivimos en un ambiente dinámico en el que las sociedades y las empresas deben aprender a desarrollarse al mismo ritmo que la tecnología que nos rodea. Los últimos diez años hemos experimentado una mutación hacia la digitalización a todos los niveles de nuestra vida. Si este venía siendo un cambio con un rumbo definido que avanzaba firmemente, la pandemia no ha hecho más que acelerarlo. El Covid-19 ha puesto de soslayo el gran margen de mejora que existe en muchas de las instituciones y empresas de nuestra sociedad, y como la digitalización puede sustituir de manera muy eficiente (tanto económicamente como operativamente) los trámites y transacciones históricamente presenciales por transacciones completamente digitales. La contrapartida de esto es la seguridad, cuanto más nos digitalizamos más información sensible dejamos en el mundo digital, y esto es algo que aprovechan los hackers. Los ataques informáticos a gobiernos y empresas están a la orden del día, evidenciando una falta de seguridad en aquellas instituciones que almacenan nuestra información más sensible. Es por ello que, al igual que avanza la tecnología, debemos hacer que avance la seguridad que la acompaña.

La tecnología Blockchain ya ha demostrado su capacidad de revolucionar por completo sectores enteros, y si bien es cierto que hay un cierto componente de burbuja en este aspecto y que esta tecnología tampoco es apta para incorporarla en todos lo que se nos ocurra, sí que hay sectores y casos en los que su aplicación sería muy beneficiosa y completamente efectiva. Este es el caso de la identidad digital. Como hemos dicho antes, cuanto más avanza la tecnología más datos se generan y más datos se requieren para que esta siga avanzando. Por ello no tiene sentido seguir confiando en sistemas de almacenamiento que no han evolucionado al mismo ritmo, y que han demostrado no ser eficientes a la hora de salvaguardar la privacidad de los usuarios.

El dato es hoy un nuevo activo financiero, generado por los usuarios, y por esta razón son estos los únicos legitimados a ser dueños de su identidad. Esto, sumado al problema de la seguridad, muestra un camino a seguir, el de otorgar al usuario la soberanía de su identidad y por ende de su información. Este nuevo concepto de identidad digital sólo puede comprenderse mediante la aplicación de una solución como el Blockchain,

pues es la única forma de satisfacer aquellos criterios que hacen de una identidad algo independiente. Estos criterios son existencia, control, acceso, transparencia, perseverancia, portabilidad, versatilidad, consentimiento, minimización y protección. Los sistemas de Self-Sovereign Identity son, hasta la fecha, los sistemas que mejor garantizan el cumplimiento de esas cualidades.

Por la propia naturaleza del Blockchain, se puede garantizar el almacenamiento seguro de la identidad en la cadena, siendo prácticamente imposible la modificación de identidades por un ente malicioso gracias a la criptografía y los mecanismos de consenso. También aporta al dueño de la identidad un control completo sobre ella, decidiendo en todo momento quien tiene acceso y a qué. Es también más eficiente, pues con una única identidad digital podemos realizar todas las transacciones y acceder a todos los servicios, en lugar de tener una identidad fragmentada y vulnerable para cada servicio.

Como sistema descentralizado, los usuarios pueden manejar su información sin la necesidad de terceros, derivando esto en menores costes de transacción. A diferencia de otros sistemas de gestión de identidad digital, el proceso de autenticación en sistemas basados en Blockchain requiere un mecanismo diferente, concretamente el mecanismo Handshake. Este consta de un proceso de tres partes, el inicio de sesión, verificar la solicitud, y dar una respuesta.

Por todas estas razones, mi conclusión es que la tecnología Blockchain está capacitada para ser aplicada en la identidad digital, mejorando ampliamente los sistemas actuales.

7. Anexo

8. Bibliografía

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Sarmah, S. S. (2018). Understanding blockchain technology. Computer Science and Engineering, 8(2), 23-29.

Kikitamara, S., van Eekelen, M. C. J. D., & Doomernik, D. I. J. P. (2017). Digital identity management on blockchain for open model energy system. Unpublished Masters thesis– Information Science.

Wadhwa, S. (2019). Decentralized digital identity management using blockchain and its implication on public sector (Doctoral dissertation, Dublin Business School).

Rodríguez, N. (2018). Historia de la tecnología Blockchain – Infografía de línea de tiempo. 101blockchains. https://101blockchains.com/es/historia-de-la-blockchain/

Java T Point. (s.f.). History of Blockchain. Java T Point. https://www.javatpoint.com/history-of-blockchain

Java T Point. (s.f.). Blockchain Merkle Trees. Java T Point. https://www.javatpoint.com/blockchain-merkle-tree

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Mendoza, F. (4 de julio de 2020). Blockchain's evolution: 1.0, 2.0, 3.0. Medium. https://medium.com/the-capital/blockchains-evolution-1-0-2-0-3-0-4fdb2c5e52be

Caballero, M., Carrera, M., Ramió, A. (2020). Finanzas descentralizadas para inquietos. Bubok editorial. Madrid.

Wegrzyn K. E., Wang, e. (2021). Types of Blockchain: Public, private, or something in between. Foley. https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

Blockchaines. (s.f.). Blockchain 3.0, el futuro. Blockchaines. https://www.blockchaines.tech/tutoriales/blockchain-3-0-el-futuro/

Data-Flair. (s.f.). Types of Blockchain – Decide which one is better for your business needs. Data-Flair. https://data-flair.training/blogs/types-of-blockchain/

Greenspan, Gideon. (2015). MultiChain Private Blockchain — White Paper. http://www.multichain.com/download/MultiChain-White-Paper.pdf.

Hyperledger. (s.f.). Blockchain technologies for business. Hyperledger. https://www.hyperledger.org

Higgins, S. (21 de julio de 2015). Inside R3CEV's Plot to Bring Distributed Ledgers to Wall Street. CoinDesk. https://www.coindesk.com/markets/2015/07/21/inside-r3cevs-plot-to-bring-distributed-ledgers-to-wall-street/

Hayes, A. (29 de junio de 2021). Target hash. Investopedia. https://www.investopedia.com/terms/t/target-hash.asp

Frankenfield, J. (13 de enero de 2022). Hash. Investopedia. https://www.investopedia.com/terms/h/hash.asp

Eremenko, K. (3 de mayo de 2018). How does Bitcoin / Blockchain mining work? Medium. https://medium.com/swlh/how-does-bitcoin-blockchain-mining-work-36db1c5cb55d

Patel, M. (11 de mayo de 2022). Consensus algorithms in blockchain. Geeks for geeks. https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/

Chaudhury, A. (7 de noviembre de 2021). What is Nakamoto consensus and how does it power Bitcoin? Bitcoin magazine. https://bitcoinmagazine.com/guides/what-is-nakamoto-consensus-bitcoin

Nester, W. (15 de noviembre de 2018). The Nakamoto consensus algorithm. Medium. https://medium.com/nakamo-to/nakamoto-consensus-21cd304f96ff

Pavel, V. (2015). Blackcoin's proof-of-stake protocol. Blackcoin whitepaper.

Xu, X., Staples, M., Weber, I. (2019). Architecture for Blockchain Applications. Springer.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., y Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Liang, Y. C. (2020). Blockchain for dynamic spectrum management. In Dynamic Spectrum Management (pp. 121-146). Springer. Singapur.

Douceur, J. R. (2002). Sybil attacks. International workshop on peer-to-peer systems. (pp. 251-260). Springer.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Disponible en el SSRN 2709713

Al-Jaroodi, J., & Mohamed, N. (Enero de 2019). Industrial applications of blockchain. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0550-0555). IEEE.

Shrier, D., Wu, W. y Pentland, A. (2016) Blockchain & infrastructure (identity, data security). Massachusetts Institute of Technology-Connection Science vol. 1, no. 3.

Minelli, M., Von Gunten, C. (2014). Chain of a lifetime: How blockchain technology might transform personal insurance. Prepared report, long finance.

Cohn, A., West, T., Parker, C. (2017). Smart after all: Blockchain, smart contracts, Parametric insurance, and smart energy grids. Georgetown law technology review. (pp 273-304).

Prisco, G. (2016). The Blockchain for healthcare: Gem launches Gem health Network with Philips Blockchain Lab. Bitcoin magazine.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

Lasseter, H., Paigi, P. (2004). Microgrid: A conceptual solution. 35th Annual Power Electronics Specialists Conference. Vol 6. (Pp 4285-4290).

Bybit learn. (18 de febrero de 2022). ¿Qué es el trilema del Blockchain? Bybit. https://learn.bybit.com/es/blockchain/el-trilema-de-la-blockchain/

Song, W., Shi, S., Xu, V., Gill, G. (21 de noviembre de 2016). Advantages and disadvantages of Blockchain technology. Blockchain technology. https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

Ferreira, M. B. (2014). Identity management for the requirements of the information security. IEEE International Conference on Industrial Engineering and Engineering Management, 53-57.

OECD. (2015). Working Party on Security and Privacy in the Digital Economy.

Kvitnitsky, A. (2018, September 17). Digital Identity: Crucial for the Success of Today's Mobile-First World. Retrieved from GSMA: https://www.gsma.com/identity/digitalidentity-crucial-for-the-success-of-todays-mobile-first-world

Erik, J. (2018, Aug). EEMA. Retrieved from EEMA: https://www.eema.org/identityblog/the-problem-of-self-sovereign-identity-we-cant-trust-people-john-erik-setsaas/

Pimenidis, E. (2010). Digital Identity Management. Bristol: University of the West of England

Miriam Lips, C. P. (2008). IDENTITY MANAGEMENT IN INFORMATION AGE GOVERNMENT. Wellington: Victoria University of Wellington

Rouse, M. (2017, Nov). Tech Target. Retrieved from Tech Target: https://searchsecurity.techtarget.com/definition/identity-management-ID-management

Yuan Cao, L. Y. (2010). A Survey of Identity Management Technology. IEEE.

Techopedia. (s.f.). Digital Identity. Techopedia. https://www.techopedia.com/definition/23915/digital-identity

Olson, E. (2016). Personal identity. The Stanford Encyclopedia of Philosophy. Edited by Zalta, Edward. N.

Ayed, G. (2014). Architecting User-centric Privacy-as-a-set-of-services: Digital Identity- related Privacy Framework. Springer.

McWaters, J. (Agosto de 2016). A blueprint for digital identity. World Economic Forum. https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Consensys. (s.f.). Blockchain in digital identity. Consensys. https://consensys.net/blockchain-use-cases/digital-identity/

Fearon, J. D. (1999). WHAT IS IDENTITY (AS WE NOW USE THE WORD)? Stanford. Stanford University.

WEF. (2018). Identity in a Digital World. Ginebra. WEF.

OECD. (2015). Working Party on Security and Privacy in the Digital Economy. OECD.

Kvitnitsky, A. (2018, September 17). Digital Identity: Crucial for the Success of Today's Mobile-First World . Retrieved from GSMA: https://www.gsma.com/identity/digital-identity-crucial-for-the-success-of-todays-mobile-first-world

Erik, J. (2018, Aug). EEMA. Retrieved from EEMA. https://www.eema.org/identityblog/the-problem-of-self-sovereign-identity-we-cant-trust-people-john-erik-setsaas/

Alliance, S. I. (2018, June 19). secureidentityalliance. Retrieved from secureidentityalliance.org: https://secureidentityalliance.org/public-resources/152-strong- identity-strong-borders-an-sia-paper-june-2017/file

United Nations. (2018). E-GOVERNMENT SURVEY 2018. New York. UNITED NATIONS.

United Nations. (2020). E-GOVERNMENT SURVEY 2020. New York: UNITED NATIONS.

Griffith, J. (2 de diciembre de 2021). What you need to know about centralized vs decentralized identity mangement. Ping Identity. https://www.pingidentity.com/en/resources/blog/post/centralized-decentralized-identity-management.html

Bernd Zwattendorfer, T. Z. (2014). An Overview of Cloud Identity Management-Models. Institute for Applied Information Processing and Communications.

Rachida AJHOUN, R. A. (2014). Towards a New Model of Management and Securing Digital Identities . IEEE.

Andrew Tobin, D. R. (2017). The Inevitable Rise of Self-Sovereign Identity. Sovrin Foundation.

World Economic Forum. (2016). A Blueprint for Digital Identity : The Role of Financial Institutions in Building Digital Identity. WEF.

Dittmar, B.C. (Noviembre de 2016). “Application of the Blockchain For Authentication and ver- ification of Identity”. http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M. (2017). Uport: A platform for self-sovereign identity. https://whitepaper.uport.me/uPortwhitepaperDRAFT20170221.pdf

Mikula, T., Jacobsen R. H. (2018). Identity and access management with blockchain in electronic healthcare records. 21st Euromicro Con- ference on Digital System Design (DSD). IEEE. pp. 699–706.

Zhao, Z., & Liu, Y. (2019, September). A blockchain based identity management system considering reputation. In 2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE) (pp. 32-36). IEEE.

Hamer, T., Taylor, K., Ng, K. S., & Tiu, A. (2019). Private Digital Identity on Blockchain. In BlockSW/CKG@ ISWC.

Allen, C. (2016). The path to Self-Sovereign Identity. Life with Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html