Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Tema

Identidad Digital Auto-Soberana

Título

Identidad digital basada en tecnología blockchain (modelo PKI descentralizado)

Autor: Ing. Gastón Alejandro Cordero
Directora del Tesis: Graciela Pataro
Año 2020
Cohorte 2015

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firmado,

Cordero, Gastón Alejandro
DNI: 31.583.761

RESUMEN

El tema de estudio será el desarrollo de una identidad digital sobre la cual el dueño sea el único que otorga y revoca derechos de lectura sobre sus documentos, que pueden ser datos personales completos/parciales y también reclamos verificables (atestaciones) sobre datos que caracterizan a la persona (por ejemplo: posee licencia de conducir, es médico, se graduó en una facultad, etc), para presentar a las instituciones con quienes desee entablar una relación.

El usuario final es el único con potestad sobre su información financiera y datos personales. Puede otorgar o revocar a las instituciones el derecho de consulta y descarga sobre cada pieza de información para su validación o utilización en operaciones previamente informadas y consentidas. La identidad digital estará implementada sobre una red blockchain, la cual permitirá la administración de la misma de forma descentralizada y sin la necesidad de un organismo central que de fe de la veracidad de los distintos atributos de una identidad, sino que la confianza estará dada por la red.

El concepto del modelo será similar a la forma en que almacenamos y gestionamos nuestras identidades no digitales. Fuera de Internet, documentos de identidad como pasaportes, certificados de nacimiento, facturas de servicios, etc., se resguardan en un lugar seguro del hogar, se comparten con terceros solo cuando es necesario, y decidimos qué tipo de información compartir. Esto es lo que denominamos identidad auto-soberana, darle al control al usuario sobre sus datos personales decidiendo qué compartir y con quién.

Esta misma forma es la que se busca replicar en el ambiente digital, con la identidad auto-soberana, y la ayuda de la tecnología blockchain. En el mundo físico, los procesos de identificación admiten el uso de atributos validados por terceros. Por ejemplo, un individuo (propietario de la identidad) quiere acceder a un establecimiento (parte que confía), donde la condición de acceso es la mayoría de edad. Saca de su billetera la licencia de conducir (el

atributo), emitida y validada por un instituto de control de vehículos (tercero) y la presenta en el establecimiento. Aunque el encargado no tiene contacto con ese tercero, da crédito a los datos que ve en la licencia de conducir, porque confía en esa institución.

El siguiente gráfico, muestra cuáles son los participantes del ecosistema del sistema de “Identidad Auto-Soberana”:

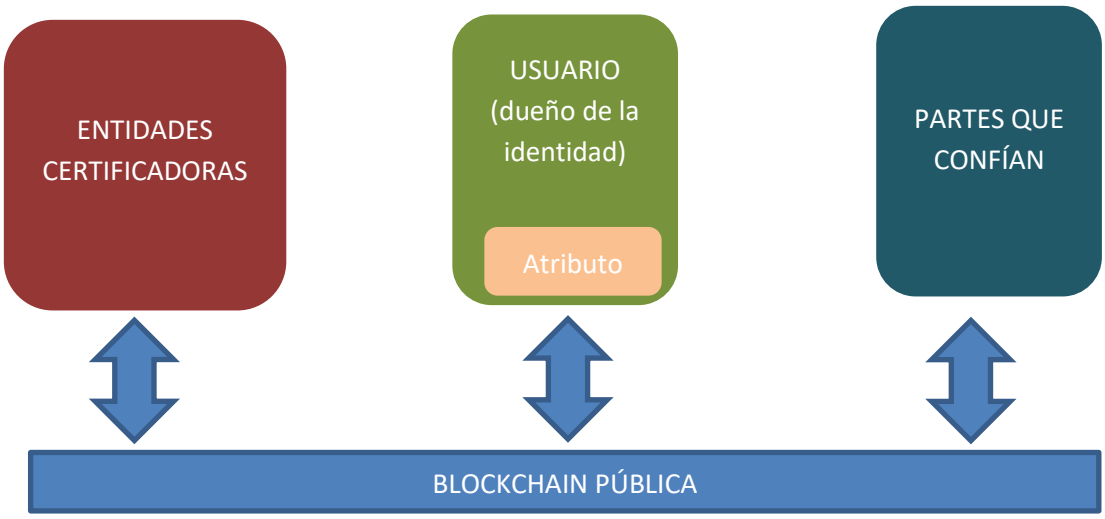

Imagen 1. Simplificación del diseño planteado (desarrollo propio).

Los usuarios son los dueños de sus identidades, estos pueden elegir hacerla pública o privada según sus preferencias individuales. Las partes que confían pueden acceder rápidamente a las solicitudes de identidad validadas y los verificadores o entidades certificadoras pueden recibir una recompensa por sus contribuciones y certificaciones.

Las entidades certificadoras o autoridades pertinentes como empresas de servicios públicos, notarios, bancos, agencias de pasaportes, hospitales, autoridades de licencias de conducir, departamentos de inmigración, pueden firmar las declaraciones del usuario.

Palabras clave

Identidad soberana, identidad digital, blockchain, entidades certificadoras.

ÍNDICE

1. PRÓLOGO

En el presente trabajo se definirá un modelo teórico sobre un sistema de gestión de identidad distribuido y descentralizado, en donde se explicarán todas las características y ventajas que dará el nuevo modelo desde el punto de vista de la seguridad de la información. Se trata de una solución para escapar de los documentos en papel y pasar a una identidad digital con privacidad, seguridad, transparencia y derechos individuales. Donde uno de principales características será el de sostener que los usuarios deben estar en el centro del proceso de gestión de identidad.

El objetivo, por tanto, de este trabajo es definir el marco conceptual de una solución integral que pone el foco en devolver la titularidad y control de los datos, y por consecuencia de la identidad, a los usuarios, al mismo tiempo les permite la plena libertad para elegir con qué institución entablar una relación, pudiendo llevarse consigo los datos y seguir operando de forma fluida y sin interrupciones mayores. El hecho de que una identidad esté descentralizada supone un gran cambio del modelo actual, en el que el usuario tenía muy poco control sobre su propia identidad. En el nuevo concepto, el ciudadano es soberano de su identidad y decide qué información quiere compartir y con quién, pudiendo asociar infinidad de atributos que podrán consumir diferentes organizaciones públicas y privadas.

2. MARCO TEÓRICO

2.1 Identidad digital

Según el modelo planteado por F. Georges, una identidad definida en el mundo digital está constituida por diferentes tipos de datos, los cuales varían en cantidad según el usuario tenga o no la intención de revelarlos. Lo que da lugar a una identidad declarada, compuesta por aquella información que revela expresamente la persona, otra identidad actuante, según las acciones que esta lleva a cabo, y otra calculada o inferida, según el análisis de las acciones que realiza la persona. Toda esta información puede ser utilizada para conformar una idea de quién es y qué le gusta a una persona determinada. [1]

Se denomina **identidad digital** a toda información electrónica asociada con un individuo en un sistema informático. Dichos sistemas de gestión de identidades, entre algunas de sus principales aplicaciones se encuentran la autenticación y autorización. Definimos a la **autenticación** al proceso de verificación de la identidad de un usuario. Una vez que dicho usuario ha sido **autenticado**, se le puede permitir o denegar el **acceso** a un conjunto de recursos, dicho proceso recibe el nombre de **autorización**.

2.2 Blockchain

Blockchain o cadena de bloques, es una tecnología que permite crear un registro distribuido de transacciones digitales mantenido por una red descentralizada de nodos. Todas las transacciones son comunicadas a todos los nodos que pertenecen a la red. Algunos de estos nodos son encargados de verificarlas (para ello debe existir un acuerdo entre la mayoría de los nodos, el método de verificación se conoce como algoritmos de consenso) y las van agrupando en bloques. De esta forma permite hacer transacciones entre dos partes sin necesidad de un intermediario.

Cada bloque se identifica por medio de un hash: un valor único calculado criptográficamente a partir del contenido del bloque, e incluye una referencia

al hash del bloque anterior, de modo que los bloques quedan enlazados, formando de esta forma la cadena de bloque. Esta cadena es en sí un registro de transacciones o libro contable (“ledger”) público, compartido por todos los nodos de la red.

La integridad de los registros reside en el consenso entre los participantes de la red (aplicando protocolos criptográficos), que reemplaza la necesidad de utilizar terceras partes de confianza que garanticen la seguridad de la información.

2.2.1 Componentes principales de una blockchain

2.2.1.1. Función Hash

Es un algoritmo matemático que calcula un valor de salida único (llamada resumen hash o compendio) para una entrada de cualquier tipo y tamaño. El tamaño del hash es fijo y se mide en cantidad de bits (en función de la implementación utilizada).

Esto permite tomar datos de entrada de forma independiente, hacer hash de estos y obtener el mismo resultado, lo que demuestra que no hubo cambios en los datos. Incluso el cambio más pequeño en la entrada (por ejemplo, el cambio de un solo bit) dará como resultado un hash completamente diferente.

Las funciones hash poseen importantes propiedades de seguridad, las cuales son:

1. Resistentes a pre-imagen: Esto significa que son unidireccionales; es computacionalmente imposible calcular el valor de entrada correcto dado un cierto valor de salida conocido (por ejemplo, dado un resumen, encuentre x tal que hash (x) = resumen).

2. Resistentes a segunda pre-imagen: Esto significa que, para una entrada conocida sea computacionalmente imposible encontrar una segunda entrada que produzca la misma salida (por ejemplo, dada x, encuentre y tal que hash (x) = hash (y)).

3. Resistentes a colisiones: Esto significa que uno no puede encontrar dos entradas que tengan la misma salida. Más específicamente, es computacionalmente imposible encontrar dos entradas que produzcan el mismo compendio (por ejemplo, encuentre una x y una y que hash (x) = hash (y)).

Dentro de una red de blockchain, las funciones de hash son utilizadas para diferentes tareas:

- Cálculo de direcciones. Generalmente, las direcciones que son utilizadas por usuarios finales en aplicaciones que utilicen servicios de una red blockchain, son generadas con datos particulares de cada usuario y su clave pública (por ejemplo, calcular el Hash de la clave pública).
- Creación de identificadores únicos.
- Protección de los datos del bloque: los nodos encargados de la publicación de bloques almacenan dentro del encabezado del bloque un resumen de los datos a publicar.
- Asegurar el encabezado de bloque: El resumen de hash del encabezado del bloque actual se incluirá en el encabezado del siguiente bloque, asegurando de esa forma los datos del encabezado del bloque actual.

Debido a que el encabezado del bloque incluye una representación de hash de los datos del bloque, los datos del bloque en sí también están protegidos cuando el resumen del encabezado del bloque se almacena en el siguiente bloque.

2.2.1.2. Número “Nonce”

Es un número arbitrario que solo se usa una vez. Puede ser combinado con datos para producir diferentes hashes, por ejemplo:

hash (data + nonce) = resultado.

Solo cambiando el valor de nonce proporciona un mecanismo para obtener diferentes valores mientras se mantienen los mismos datos.

2.2.1.3. Transacciones:

Una transacción representa una interacción entre las partes. En algunas implementaciones de blockchain, un suministro constante de nuevos bloques (incluso con cero transacciones) es fundamental para mantener la seguridad de la red; evitando de esta forma que los usuarios malintencionados se "pongan al día" y fabriquen una cadena de bloques alterada más larga.

2.1.2.4. Criptografía de clave asimétrica (clave pública):

La criptografía de clave asimétrica utiliza un par de claves: una clave pública y una clave privada que están matemáticamente relacionadas entre sí. La clave pública se hace pública sin reducir la seguridad del proceso, pero la clave privada debe permanecer secreta así los datos pueden conservar su protección criptográfica.

A pesar de que existe una relación entre las dos claves, la clave privada no se puede determinar de manera eficiente desde el conocimiento de la clave pública. Uno puede cifrar con una clave privada y luego descifrar con la clave pública. Alternativamente, uno puede cifrar con una clave pública y luego descifrar con una clave privada.

Dentro de una red de blockchain, se les puede dar los siguientes usos a la criptografía de clave asimétrica, por ejemplo:

- Las claves privadas son utilizadas para firmar transacciones digitalmente.
- Las claves públicas son utilizadas para calcular direcciones.
- Las claves públicas son utilizadas para verificar las firmas generadas con claves privadas.
- Brinda la capacidad de verificar que el usuario que transfiere valor a otro usuario está en posesión de la clave privada capaz de firmar la transacción.

2.1.2.5. Direcciones y derivación de direcciones

Algunas redes utilizan una dirección, que es una cadena de caracteres alfanumérica corta derivada de la clave pública del usuario que utiliza una

función criptográfica hash, junto con algunos datos adicionales (por ejemplo, número de versión, sumas de comprobación).

La mayoría de las implementaciones de blockchain utilizan direcciones como los puntos finales "para" y "desde" en una transacción. Las direcciones son más cortas que las claves públicas y no son secretas. Un método para generar una dirección es crear una clave pública, aplicándole una función criptográfica de hash y convirtiendo el hash en texto:

clave pública → función hash criptográfica → dirección

Cada implementación de blockchain puede implementar un método diferente para derivar una dirección.

2.1.2.6. Bloque

Un bloque representa una lista de transacciones grabada en un registro a lo largo de un período de tiempo determinado. El tamaño, período y el evento disparador de los bloques varía en cada red. Los usuarios envían transacciones candidatas a publicarse a la red blockchain mediante software (aplicaciones de escritorio, aplicaciones para teléfonos inteligentes, billeteras digitales, servicios web, etc.). El software envía estas transacciones a un nodo o nodos dentro de la red de blockchain.

Las transacciones se agregan a la cadena de bloques cuando un nodo de publicación publica un bloque. Un bloque está compuesto por un encabezado y por los datos que se quieren publicar.

El encabezado contiene información sobre el bloque en sí (metadatos del bloque), que normalmente incluye:

- El número de bloque, también conocido como altura de bloque en algunas redes.
- El valor hash del encabezado del bloque anterior.
- Una representación de hash de los datos del bloque (existen diferentes métodos para lograr esto, como generar un árbol Merkle y almacenar el hash raíz, o utilizar un hash de todos los datos del bloque).
- Una marca de tiempo (timestamp).

- El tamaño del bloque.
- El valor llamado “nonce”. (En algunas redes que utilizan el algoritmo de consenso basado en minería, este número es manipulado por el nodo de publicación. Otras redes pueden o no incluirlo o usarlo para otro propósito que no sea resolver un problema de hash).

El árbol Merkle es una estructura de datos que relaciona un conjunto de transacciones y las agrupa entre pares para obtener un único hash (raíz), con el objetivo de disminuir tiempos y recursos en la verificación de integridad de una gran cantidad de información.

El hash raíz se crea agrupando todos los hashes de las transacciones en pares a los que, a su vez, les será aplicada de nuevo la función hash criptográfica pertinente para crear un nuevo hash que equivale a ambos. Si acaso el número de entradas fuera impar, la última se copiaría a sí misma y se emparejaría con esa copia para permitir el proceso. Los hashes resultantes volverán a organizarse por pares y a repetir la misma técnica, hasta que sólo quede una única línea hash como resumen de todas las que pasaron por este proceso de fusión. Entonces, por ejemplo, si tuviéramos un bloque que contiene 512 transacciones, el árbol de Merkle se encargaría de agruparlas en 256 pares, que se reducirían luego a 128, luego a 64, después 32, 16, 8, 4, 2 y la última. Una sola línea alfanumérica se queda allí para representar esas 512 transacciones, en lugar de recargar el bloque con 512 hashes. Por otro lado, para el caso de la red “Ethereum” [1] se utiliza el Árbol de Patricia, que es concretamente aplicar un árbol de Merkle para tres diferentes partes que componen la red, que son Transacciones, Estados y Recibos de ejecución de contratos inteligentes.

[1] De https://www.ethereum.org/: “Lanzado en 2015, Ethereum es la cadena de bloques programable líder en el mundo. Al igual que otras cadenas de bloques, Ethereum tiene una criptomoneda nativa llamada Ether (ETH). Pero a diferencia de otras cadenas de bloques, Ethereum puede hacer mucho más. Ethereum es programable, lo que significa que los desarrolladores pueden usarlo para crear nuevos tipos de aplicaciones.”

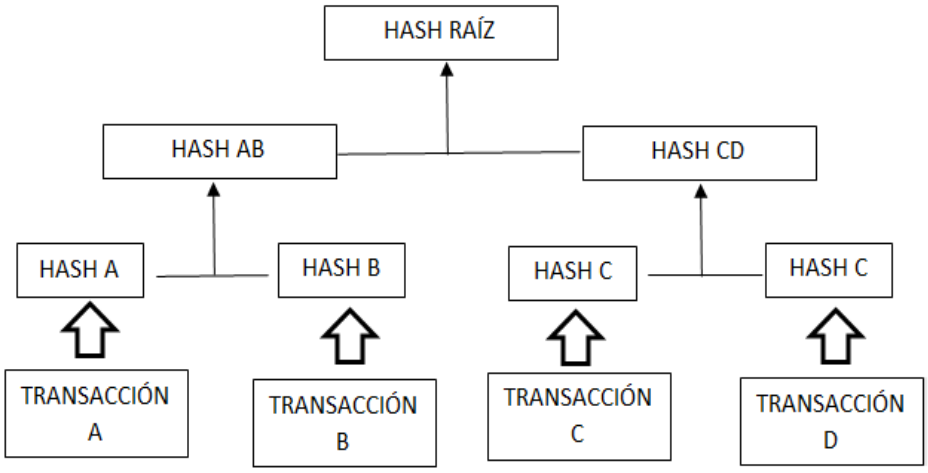

Imagen 2. Ejemplo del árbol de merkle. (desarrollo propio).

Con esto es posible garantizar la integridad de los elementos de un conjunto. Reduciendo significativamente la cantidad de datos que deben mantenerse para fines de verificación, separando de esta forma la validación de los datos de los propios datos.

La sección de datos contiene una lista de transacciones validadas y auténticas que se han enviado a la red de blockchain.

2.1.2.7. Cadena

Los bloques se encadenan a través de cada bloque que contiene el hash del encabezado del bloque anterior, formando así la cadena de bloques. Si se cambiara un bloque previamente publicado, tendría un hash diferente. Esto, a su vez, causaría que todos los bloques subsiguientes también tengan hashes diferentes, ya que incluyen el hash del bloque anterior. Esto hace posible detectar y rechazar fácilmente los bloques alterados.

2.1.2.8. Red

La red está compuesta de nodos, que cada uno de ellos es una computadora que ejecuta un algoritmo diseñado para asegurar la red. Cada nodo contiene un registro completo de todas las transacciones grabadas en la blockchain. Los nodos pueden estar ubicados en cualquier lugar del mundo y pueden ser operados por cualquier persona y reciben un incentivo para

operar el nodo. El algoritmo subyacente de la blockchain los recompensa por su servicio.

2.1.2.8.1. Categorías

Los distintos tipos de redes pueden clasificarse según el acceso a los datos o según los permisos para generar bloques:

Según los permisos:

Sin permisos: en estas no hay restricciones para que los participantes puedan procesar transacciones y crear bloques. Son por lo general, de código abierto, disponibles de forma gratuita para cualquier persona que desee descargarlas. Dado que cualquier persona tiene derecho a publicar bloques, esto se traduce en la propiedad de que cualquiera puede leer la cadena de bloques, así como emitir transacciones en la cadena de bloques (al incluir esas transacciones dentro de los bloques publicados).
Dado que las redes de blockchain sin permiso están abiertas para que todos puedan participar, los usuarios malintencionados pueden intentar publicar bloques de forma mal intencionada. Para evitar esto, las redes de blockchain sin permiso a menudo utilizan un acuerdo multipartito o un sistema de "consenso" que requiere que los usuarios gasten o mantengan recursos cuando intentan publicar bloques. Esto evita que los usuarios malintencionados subviertan fácilmente el sistema.

Con permisos: son aquellas en las que los usuarios que publican bloques deben ser autorizados por alguna autoridad. Dado que solo los usuarios autorizados mantienen la cadena de bloques, es posible restringir el acceso de lectura y restringir quién puede emitir transacciones. Este tipo de redes pueden permitir que cualquiera lea los bloques o pueden restringir el acceso de lectura a personas autorizadas. También pueden permitir que cualquiera que envíe transacciones se incluya en la cadena de bloques o, de nuevo, pueden restringir este acceso solo a personas autorizadas. También utilizan modelos de consenso para la publicación de bloques, pero estos métodos a menudo no requieren el gasto o el mantenimiento de recursos. Esto se debe a que se requiere el establecimiento de la identidad de cada uno para participar como miembro de la red de blockchain autorizada; los que

mantienen la cadena de bloques tienen un nivel de confianza mutuo, ya que todos estaban autorizados para publicar bloques y la autorización puede revocarse si realizan algo mal intencionado. Los modelos de consenso en este tipo de redes son generalmente más rápidos y menos costosos computacionalmente.

Más allá de la confianza, estas redes brindan transparencia y conocimiento que pueden ayudar a informar mejor las decisiones comerciales y responsabilizar a las personas que se comportan mal. Esto puede incluir explícitamente a las entidades de auditoría y supervisión, lo que hace que las auditorías sean una ocurrencia constante en lugar de un evento periódico.

2.1.2.9. Algoritmo de consenso

Uno de los aspectos importes de la tecnología blockchain es determinar qué usuario publica el siguiente bloque. Esto se resuelve mediante la implementación de uno de los muchos modelos de consenso posibles. En tal situación, se nos presentan los siguientes inconvenientes: ¿Por qué un usuario propagaría un bloque que otro usuario está intentando publicar? ¿Quién resuelve los conflictos cuando varios nodos publican un bloque aproximadamente al mismo tiempo? Para hacer que esto funcione, se utilizan modelos de consenso para permitir que un grupo de usuarios que desconfían mutuamente trabajen juntos.

La integridad se logra utilizando complejos protocolos, conocidos como mecanismo de consenso que permiten, por un lado, detectar cambios en los datos y, por otro, asegurar que todos los nodos de la red comparten una misma versión de los datos y que no es posible introducir información falsa en la cadena sin hacerse del control de una parte significativa de los nodos.

No obstante, independientemente del modelo, cada bloque debe ser válido y, por lo tanto, cada usuario de la red de blockchain puede validarlo de manera independiente. Al combinar el estado inicial y la capacidad de verificar cada bloque desde ese momento, los usuarios pueden acordar independientemente el estado actual de la cadena de bloques.

Se puede presentar la situación que se generen dos cadenas válidas a un nodo, el mecanismo predeterminado en la mayoría de las redes es que la cadena "más larga" se ve como la correcta y se adoptará; esto es porque se ha dedicado la mayor cantidad de trabajo en ella.

Para las redes blockchain sin permiso, generalmente hay muchos nodos de publicación que compiten al mismo tiempo para publicar el siguiente bloque. Por lo general, hacen esto para ganar la criptomoneda y/o las tarifas de transacción. Son usuarios que desconfían mutuamente y que solo pueden conocerse entre sí por sus direcciones públicas. Es probable que cada nodo de publicación esté motivado por un deseo de ganancia financiera, no por el bienestar de los otros nodos de publicación o incluso por la propia red.

Para las redes de blockchain con permiso se pueden usar distintos recursos para validar si un usuario actúa de forma maliciosa y luego poder efectuar algún tipo de sanción. Y en algunas de ellas, puede existir cierto nivel de confianza entre los nodos de publicación. En este caso, es posible que no exista la necesidad de un modelo de consenso con uso intensivo de recursos (tiempo de cálculo, inversión, etc.) para determinar qué participante agrega el siguiente bloque a la cadena.

Generalmente, a medida que aumenta el nivel de confianza, la necesidad del uso de recursos como medida para generar confianza disminuye. Para algunas implementaciones de blockchain con permiso, la visión de consenso va más allá de garantizar la validez y autenticidad de los bloques, pero abarca todos los sistemas de controles y validaciones desde la propuesta de una transacción hasta su inclusión final en un bloque. En este trabajo se mencionarán algunos de los principales algoritmos de consenso que se conocen:

1. Prueba de trabajo (PoW): Un usuario de la red está habilitado a publicar el siguiente bloque debido a que es el primero en resolver un problema matemático el cual requiere una gran cantidad de poder de cálculo. La solución a este rompecabezas es la "prueba" de que se ha realizado el trabajo. El rompecabezas está diseñado de tal manera que resolverlo es difícil, pero verificar que una solución sea válida es fácil. Esto permite que todos los

demás nodos validen fácilmente los siguientes bloques propuestos, y cualquier bloque propuesto que no satisfaga el enigma se rechazaría.

El problema computacional (rompecabezas) utilizado es requerir que el resumen de hash de un encabezado de bloque sea menor que un valor objetivo. Para generar un bloque de manera exitosa, es necesario ajustar el encabezado del bloque de tal manera que sea menor o igual que el objetivo (Hash). Se llega a este hash en particular, variando una pequeña porción del encabezado del bloque, llamado “nonce”. Un nonce siempre comienza con “0” y se incrementa cada vez para obtener el hash requerido.

Por ejemplo, Bitcoin, que utiliza este algoritmo, **ajusta la dificultad del rompecabezas cada 2016 bloques** para influir en la tasa de publicación de bloques para que esté alrededor de una vez cada diez minutos. El ajuste del nivel de dificultad del rompecabezas básicamente se realiza aumentando o disminuyendo el número de ceros iniciales requeridos. Al aumentar el número de ceros iniciales, aumenta la dificultad del rompecabezas, porque cualquier solución debe ser menor que el nivel de dificultad, lo que significa que hay menos soluciones posibles. Este ajuste es para mantener la dificultad de cálculo del rompecabezas y, por lo tanto, para mantener el mecanismo de seguridad central de la red Bitcoin. La potencia de cómputo disponible aumenta con el tiempo, al igual que la cantidad de nodos de publicación, por lo que la dificultad del rompecabezas generalmente aumenta.

Un aspecto importante de este modelo es que el trabajo puesto en un rompecabezas no influye en la probabilidad de que uno resuelva los rompecabezas actuales o futuros porque los rompecabezas son independientes. Esto significa que cuando un usuario recibe un bloque válido de otro usuario, se los incentiva a descartar su trabajo actual y a comenzar a construir el nuevo bloque porque saben que los otros nodos de publicación se construirán a partir de él.

El modelo penaliza las decisiones erradas, si un nodo se aferra a un determinado estado de la red, y luego resulta que no estuvo alineado con el resto de nodos, entonces todo el trabajo del nodo ha sido en vano y no recibirá una recompensa.

La convención es que **la cadena más larga –más pesada– siempre refleja 'la verdad' del estado de la red**, debido a que es probable que en ella se haya invertido más trabajo –capacidad informática que consume mucha energía eléctrica– para resolver las complejas operaciones matemáticas. Las cadenas más cortas –o livianas– serán rechazadas.

Una vez que un nodo de publicación ha realizado este trabajo, envían su bloque válido a los demás nodos en la red de blockchain. Los nodos del destinatario verifican que el nuevo bloque cumpla con el requisito del rompecabezas y luego agregan el bloque a su copia de la cadena de bloques. De esta manera, el nuevo bloque se distribuye rápidamente a través de la red de nodos participantes. La verificación del resultado es fácil ya que solo se necesita hacer un solo hash para verificar si resuelve el enigma.

El uso de un rompecabezas computacionalmente difícil ayuda a combatir el "Ataque de Sybil", un ataque de seguridad informática (no limitado a redes de cadena de bloques) donde un atacante puede crear muchos nodos (es decir, crear identidades múltiples) para ganar influencia y ejercer control. Este tipo de ataques se evitan requiriendo que la capacidad de generación de bloques sea proporcional a la potencia computacional disponible (que cuesta dinero). De esa manera, un adversario está limitado en la cantidad de bloques que pueden producir.

2. Prueba de participación: Su creación fue el resultado de considerar el algoritmo de prueba de trabajo como un desperdicio de recursos, ya que los costos necesarios para su ejecución resultan elevados. Para este algoritmo en particular es más relevante la cantidad de monedas almacenadas en el sistema, lo que supone un interés por parte de la comunidad en que su rendimiento sea óptimo (evitando así la confianza que da la cantidad de trabajo invertido). Por lo tanto, la probabilidad de que un usuario de la red publique un nuevo bloque está ligada a la proporción de su participación con respecto a la cantidad total de la criptomoneda apostada en la misma.

Con este modelo de consenso, no hay necesidad de realizar cálculos de recursos intensivos (que involucren tiempo, electricidad y capacidad de procesamiento). Dado que este modelo de consenso utiliza menos recursos,

algunas redes han decidido renunciar a una recompensa de creación de bloque; estos sistemas están diseñados para que toda la criptomoneda se distribuya entre los usuarios en lugar de que la nueva criptomoneda se genere a un ritmo constante. En tales sistemas, la recompensa por publicación de un bloque es generalmente la ganancia de las tarifas de transacción provistas por el usuario.

3. Prueba de tiempo transcurrido (PoET): En este algoritmo de consenso, llamado prueba de tiempo transcurrido (PoET), cada nodo de publicación solicita un tiempo de espera de una fuente de tiempo de hardware segura. Dicha fuente de tiempo es la encargada de generar tiempos aleatorios de espera y luego devolverlos al nodo de publicación. Los nodos de publicación toman el tiempo aleatorio que se les asignó y quedan inactivos durante ese tiempo. Una vez que un nodo de publicación se despierta del estado inactivo, crea y publica un bloque en la red, alertando a los otros nodos del nuevo bloque; cualquier nodo de publicación que aún esté inactivo dejará de esperar y todo el proceso comenzará de nuevo.

En lugar de competir para resolver un desafío criptográfico y publicar el próximo bloque, como sucede en Bitcoin, dicho algoritmo es una combinación de una lotería aleatoria y de un orden de llegada. Cada nodo recibe un tiempo de espera aleatorio. El que posea el menor tiempo de espera es el que está habilitado para crear el siguiente bloque de la cadena.

Este modelo requiere asegurar que se usó un tiempo aleatorio, ya que, si el tiempo de espera no se seleccionó al azar, un nodo de publicación malicioso solo esperaría la cantidad mínima de tiempo por defecto para dominar el sistema. Este modelo también requiere asegurarse de que el nodo de publicación haya esperado el tiempo real y no haya comenzado antes. Estos requisitos se resuelven ejecutando software en un entorno de ejecución confiable que se encuentra en algunos procesadores de computadora. Un nodo de publicación consultará el software que se ejecuta en este entorno seguro durante un tiempo aleatorio y luego esperará a que pase ese tiempo.

4. Round Robin: Es un modelo utilizado por algunas redes permisionadas. Dentro de este modelo los nodos se turnan para crear bloques. Round Robin tiene una larga historia basada en la arquitectura de sistemas distribuidos. Para manejar situaciones donde un nodo de publicación no está disponible para publicar un bloque en su turno, estos sistemas pueden incluir un límite de tiempo para permitir que los nodos disponibles publiquen bloques para que los nodos no disponibles no detengan la publicación. Este modelo asegura que ningún nodo crea la mayoría de los bloques. Se beneficia de un enfoque sencillo, carece de problemas criptográficos y tiene bajos requisitos de potencia. Dado que existe una necesidad de confianza entre los nodos, este modelo no funciona bien en las redes blockchain sin permiso utilizadas por la mayoría de las criptomonedas. Esto se debe a que los nodos maliciosos podrían agregar continuamente nodos adicionales para aumentar sus probabilidades de publicar nuevos bloques. [5]

3. MODELO DE IDENTIDAD AUTO - SOBERANA

En la actualidad los sistemas de gestión de identidades funcionan de forma centralizada, en donde los datos relacionados con identidades son manejados por una parte central de confianza en nombre de los propietarios de las mismas. También, los esquemas de autenticación de identidad utilizados se basan en el cifrado asimétrico y el uso de un modelo de confianza centralizado. La infraestructura de clave pública (PKI) implementa este modelo de confianza centralizado focalizando la dependencia en una jerarquía de autoridades de certificación. Dichas autoridades de certificación establecen la autenticidad de la vinculación entre una clave pública y su propietario a través de la emisión de certificados digitales.

Para entender mejor cuales son las amenazas a las cuales se enfrentan en la actualidad este tipo de sistemas, se enumerarán una serie de incidentes que se produjeron en los últimos años los cuales afectaron de forma directa a la privacidad:

- se encendieron las alarmas respecto a la manera en que se gestiona la información personal en Internet, cuando Facebook (el cual cuenta con más de 2 mil millones de usuarios a nivel mundial) se vio envuelto en un escándalo de fuga de información, que afectó a más de 87 millones de personas. En este hecho estuvo implicada la firma inglesa Cambridge Analytica, la cual utilizó una aplicación en la plataforma de Facebook para obtener información relevante de los usuarios y usarla sin consentimiento para crear propaganda e influir en procesos electorales en varios países;
- la Agencia Española de Protección de Datos (AEPD) multó a Facebook por el uso indebido de datos personales con la compra de WhatsApp, debido a que se dieron a conocer los mismos sin haber obtenido un consentimiento válido de los usuarios;
- el intercambio ilegal de datos de pacientes de DeepMind.

En los incidentes antes mencionados y en otros que han ocurrido en los últimos años, los propietarios de identidades no tienen conocimiento acerca del uso ilegal de las mismas, debido a que no poseen las herramientas suficientes y adecuadas para lograr imaginar lo que sucede dentro de los sistemas y las redes por las cuales viajan sus identidades.

Dentro de este contexto, podemos decir que es necesario el uso de la tecnología Blockchain, ya que ha demostrado ser resistente a alteraciones y transparente por definición. Proporcionando seguridad gracias a su descentralización de la confianza y a su naturaliza distribuida, eliminando el riesgo de posibles errores humanos, prescindiendo de intermediarios y protegiéndose contra ciberataques. Los sistemas de gestión de identidades convencionales se basan en autoridades centralizadas, como pueden ser autoridades de certificación (CA) o registros de nombres de dominio. Desde el punto de vista de la verificación de confianza criptográfica, cada una de estas autoridades centralizadas sirve como su propia raíz de confianza. Los modelos de identidad tienden a una concepción estática del individuo o crean su perfil en relación con una única institución. Al ser iniciativas particulares de cada empresa, su escalabilidad es limitada y tiende a generar problemas para el usuario, quien está en el centro de todas estas propuestas y termina

construyendo un perfil completo con **requerimientos únicos para cada organización con la que se relaciona**, de esta formar se ve obligado a la creación de múltiples perfiles. Estos perfiles esta expuestos a ser capturados por terceros que vulneran las bases de datos de aquellas instituciones.

El control de la identidad a las autoridades centralizadas del mundo sufre los mismos problemas causados por las autoridades del mundo físico: los usuarios están sujetos a una sola autoridad que puede negar su identidad o incluso confirmar una identidad falsa. La centralización otorga de manera innata el poder a las entidades centralizadas, no a los usuarios.

3.1 Elementos claves del modelo

En esta parte del trabajo se explicará en detalle cuales son los componentes vitales del modelo, definiendo en otras cosas el papel que desempeñan:

3.1.1 Credencial digital verificable

Se utilizarán las credenciales firmadas digitalmente que fueron estandarizadas por el World Wide Web Consortium (W3C)2, con el objetivo de proporcionar una forma uniforme de expresar credenciales en la web de manera criptográficamente segura, respetando la privacidad y digitalmente verificables. Se define a las credenciales como un conjunto de afirmaciones y metadatos a prueba de manipulación que demuestran criptográficamente quién la emitió.

Según el W3C, en el mundo físico, una credencial puede consistir en:

- Información relacionada con la identificación del sujeto (por ejemplo: una foto, nombre o número de identificación).
- Información relacionada con la autoridad emisora (por ejemplo: un gobierno municipal, agencia nacional u organismo de certificación).

[2] El World Wide Web Consortium (W3C) es una comunidad internacional que desarrolla estándares que aseguran el crecimiento de la Web a largo plazo.

- Información relacionada con el tipo de credencial (por ejemplo: documento de identidad, pasaporte, licencia de conducir o una tarjeta de seguro de salud).
- Información relacionada con los atributos o propiedades específicas que la autoridad emisora afirma sobre el tema (por ejemplo: nacionalidad, clases de vehículos con derecho a conducir o fecha de nacimiento).
- Evidencia relacionada con cómo se obtuvo la credencial.
- Información relacionada con restricciones en la credencial (por ejemplo, fecha de vencimiento o términos de uso). [2]

Por lo cual, una credencial digital es capaz de representar la misma información que una credencial física. Con la incorporación de la tecnología, como las firmas digitales, se puede hacer que las credenciales sean más manipulables y más confiables que sus contrapartes físicas. Además, una de las características más importantes, es que los titulares de credenciales digitales pueden generar presentaciones verificables sobre estas y luego compartir estas presentaciones con los verificadores para demostrar que poseen credenciales con ciertas características.

Según el modelo de datos definido por el W3C, una credencial digital está compuesta por:

1- Identificador.
2- Metadatos (propiedades como: el emisor, la fecha y hora de vencimiento, una imagen representativa, una clave pública para usar con fines de verificación, el mecanismo de revocación, entre otros).
3- Reclamos verificables.
4- Pruebas.

Algunos de los ejemplos de este tipo de credenciales, pueden ser: tarjetas de identificación de empleados digitales, certificados de nacimiento digitales, certificados educativos digitales, entre otros.

Es posible tener una credencial, como un certificado de matrimonio, que contenga múltiples reclamos sobre diferentes temas que no requieren estar

relacionados. En otros casos, una credencial puede que no contenga ningún reclamo sobre la entidad a la que se emitió la credencial. Por ejemplo, una credencial que solo contiene reclamos sobre una mascota que posee una persona, pero que se emiten a nombre de su propietario.

3.1.2 Presentaciones verificables

Una presentación verificable expresa datos de una o más credenciales digitales y se presenta de manera que la autoría de los datos sea verificable. La información en una presentación en general se refiere a temas sobre el mismo tipo, pero es emitida por múltiples emisores. Es decir, si una credencial se presenta directamente, se convierte en una presentación.

De esta forma es posible, seleccionar que datos mostrar, por ejemplo, solo la información que muestra que tiene al menos 21 años de edad sin dar acceso a su dirección o nombre completo cuando intenta comprar una bebida alcohólica. Esta expresión de un subconjunto de la persona se llama **presentación verificable**. Una persona puede tener diferentes personas, por ejemplo, su persona profesional, su persona de juego en línea, su persona familiar o una persona de incógnito.

Una de las premisas de este modelo es la de mejorar la privacidad, lo cual, es importante que las entidades/sistemas que desarrollen/usen esta tecnología puedan expresar solo las partes de su personalidad que sean apropiadas para una situación específica.

3.1.3 Reclamos verificables

Un elemento vital en el modelo son los **reclamos verificables** los cuales son una forma estándar de definir, intercambiar y verificar las credenciales digitales que posee una persona. La fortaleza de la reclamación depende del grado de confianza que el verificador tiene en el emisor. Por ejemplo, si una entidad financiera emite un reclamo, en donde afirma que un usuario es poseedor de un cierto número de tarjeta de crédito, un comerciante

puede confiar en el reclamo si el comerciante tiene un alto grado de confianza en dicha entidad.

Un reclamo es una declaración sobre un tema. Un tema es algo sobre lo que se pueden hacer afirmaciones. Las reclamaciones se expresan utilizando relaciones sujeto-propiedad-valor. Por ejemplo, si alguien se graduó de una universidad en particular se puede expresar de la siguiente manera:

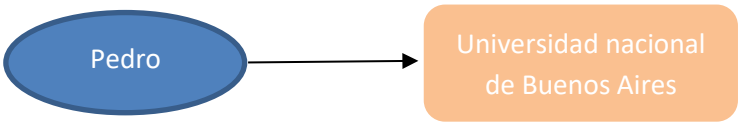

Imagen 3. Ejemplo de reclamo verificable (desarrollo propio).

La entidad que realiza el reclamo se llama **Emisor**. La entidad que posee el reclamo emitido se llama **Titular**.

Dicho esto, se puede precisar que el ciclo de vida de las credenciales y presentaciones en el ecosistema de credenciales verificables a menudo toma un camino común:

1. Emisión de una o más credenciales verificables.
2. Almacenamiento de credenciales verificables en un repositorio de credenciales (aplicación específica desarrollada para el almacenamiento de credenciales, como puede ser una billetera digital).
3. Composición de credenciales verificables en una presentación verificable para verificadores.
4. Verificación de la presentación verificable por parte del verificador.

3.2 Ecosistema de las credenciales digitales verificables

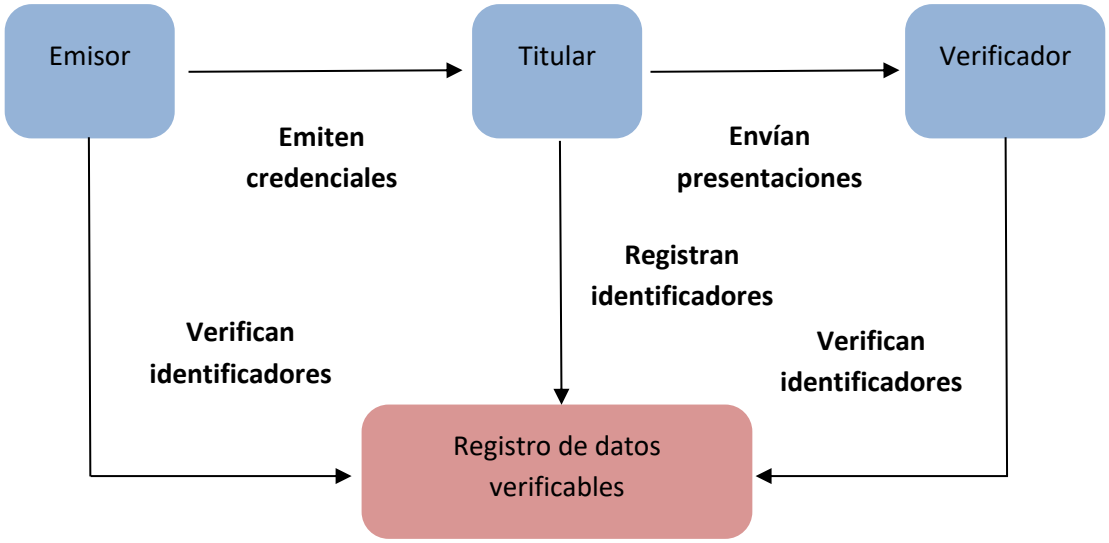

Imagen 4. Roles y flujos de información que forman la base del estándar. (desarrollo propio).

Teniendo en cuenta lo definido en el documento publicado por la W3C, los roles y relaciones que existen entre los principales actores del ecosistema de credenciales verificables son:

Emisor: es el rol que desempeña una entidad al hacer valer reclamos sobre uno o más sujetos, **crear una credencial verificable a partir de estos reclamos y transmitir la credencial verificable a un titular**. Los emisores, por ejemplo, incluyen: corporaciones, organizaciones sin fines de lucro, asociaciones comerciales, gobiernos e individuos.

Titular: es el rol que una entidad/persona desempeña al **poseer una o más credenciales verificables y puede generar presentaciones verificables (reclamos) a partir de ellas**. Los titulares, por ejemplo, pueden ser: estudiantes, empleados o clientes. Los titulares pueden presentar presentaciones verificables a cualquier verificador sin afectar la autenticidad de los reclamos y sin revelar esa acción al emisor.

Sujeto: es una **entidad sobre la cual se hacen reclamos**. Los sujetos, por ejemplo, incluyen: seres humanos, animales y cosas. En muchos casos, el titular de una credencial verificable es el sujeto, pero en algunos casos no lo es. Por ejemplo, un padre (el titular) podría tener las credenciales verificables de un niño (el sujeto), o el dueño de una mascota (el titular) podría tener las credenciales verificables de su mascota (el sujeto).

Verificador: es el rol que desempeña una entidad al **recibir una o más credenciales verificables**, opcionalmente dentro de una presentación verificable, **para su procesamiento**. Los verificadores, por ejemplo, incluyen: empleadores, personal de seguridad y sitios web.

Registro de datos verificables: es un rol que un sistema podría desempeñar mediante la mediación en la creación y verificación de identificadores, claves y otros datos relevantes, como esquemas de credenciales verificables, registros de revocación, claves públicas del emisor, etc., que podrían requerirse para usar credenciales verificables. Algunas configuraciones pueden requerir identificadores correlacionales para los sujetos. Los registros de datos verificables incluyen bases de datos confiables, bases de datos descentralizadas y redes blockchain. A menudo hay más de un tipo de registro de datos verificables utilizado en un ecosistema.

Un emisor puede emitir una credencial verificable al titular. El titular posee un identificador que también está registrado en el registro y se utiliza para autenticar contra el emisor. Después de la emisión, el titular almacena la credencial verificable. En caso de que se requiera que use la información de sus credenciales verificables, crea una presentación verificable que idealmente contiene solo la información mínima requerida.

Cada credencial verificable **contiene pruebas del emisor** (una o más firmas digitales del emisor). Estas pruebas **son parte de la presentación verificable y permiten verificar la autenticidad de los datos proporcionados** de la presentación. El verificador comprueba los identificadores y las pruebas de la presentación sin interacción con el emisor,

ya que toda la información necesaria es accesible desde el registro. Sin embargo, requiere conocimiento y registro de la identidad del emisor.

3.3 Infraestructura de clave pública descentralizada (DPKI)

Frente a este nuevo proceso, el problema que se presenta es el siguiente: generar un proceso común para la verificación de las firmas digitales de los emisores de credenciales. La respuesta habitual ha sido PKI. La premisa de la criptografía de clave pública es que cualquier persona puede verificar una firma digital de otra persona siempre que tenga acceso a su clave pública. Las dos claves están vinculadas criptográficamente, de modo que cada clave privada tiene solo una clave pública y viceversa.

En el mundo digital las comunicaciones e interacciones se aseguran mediante cifrado asimétrico, que requiere un mecanismo de intercambio seguro de claves públicas. El remitente y el receptor intercambian sus claves públicas, y luego cifran sus mensajes con la clave pública de la contraparte y descifran los mensajes con su clave privada. Sin embargo, falta un elemento. El dilema aquí es saber si las partes se comunican con la contraparte correcta. La infraestructura de clave pública (PKI) permite la confianza y la prueba de identidad al involucrar el uso de certificados y terceros de confianza. Las autoridades de certificación (CA) emiten un certificado que permite validar la integridad y la propiedad de las claves públicas.

El propietario de una clave privada, como por ejemplo un sitio web, entrega su clave pública a una Autoridad Certificante (CA) para que la firme con su propia clave privada y emitir así un certificado de clave pública. Eso es lo que verifica el navegador cada vez que se conecta a un sitio web que ofrece una conexión HTTPS cifrada. De esta forma, sabemos que estamos ingresando a un sitio seguro. Lo que hace una CA es que funciona como un tercero confiable que distribuye y administra certificados digitales para una red de usuarios. La mayoría de los servicios web están protegidos mediante la creación de las claves firmadas por las CA.

En dicho esquema, la inserción de un intermediario en la infraestructura de confianza es una vulnerabilidad. Si una CA comete un error en un certificado digital, o si su servicio se cae o tiene vulnerabilidades de seguridad, o si aumentan sus precios, o si salen del negocio, todo el sistema se ve afectado. Es la centralización de este tipo la que puede llevar a puntos únicos de falla.

Una posible solución a este inconveniente, y es la que se definirá en el presente trabajo, es la utilización de la tecnología blockchain. En donde, una red blockchain pública es una raíz descentralizada de confianza en donde nadie es el administrador pero que todos pueden usar. El enfoque descentralizado de PKI (DPKI) aborda estos problemas al difundir la confianza en todas las entidades participantes, lo que evita la necesidad de autoridades centralizadas, por lo tanto, ninguna parte maliciosa puede comprometer la integridad del sistema. En este modelo se propone el control directo y la posesión de un identificador legible globalmente para el propietario de la identidad al registrar el identificador y las claves públicas asociadas al mismo en una cadena de bloques. Cada participante tiene la misma vista en la cadena de bloques y puede vincular el valor de búsqueda de un identificador con las últimas claves públicas.

Con la tecnología Blockchain, se utiliza un algoritmo de consenso que opera en muchas máquinas diferentes y es replicado por muchas entidades diferentes en una red descentralizada. Independientemente de cual red se utilice, en todas las redes blockchain se pueden definir conceptos que podrán ser utilizados en el presente modelo:

1. Cada transacción en la cadena de bloques está firmada digitalmente por el originador.
2. Cada transacción, individualmente o en bloques, se encadena a la anterior a través de un hash digital.
3. Las transacciones validadas se replican en todas las máquinas utilizando un algoritmo de consenso (los cuales fueron explicados con anterioridad).

El resultado de esto es un registro criptográfico inmutable que hace que sea muy difícil, sino casi imposible, cambiar las transacciones pasadas o controlar maliciosamente las futuras.

Por lo tanto, una red blockchain es la correcta opción para generar registros de autoservicio descentralizado para claves públicas. Dado que cada transacción en una cadena de bloques tiene una firma digital que requiere una clave privada, es una opción válida **utilizar la propia cadena de bloques para el almacenamiento de la clave pública asociada**, o cualquier otra clave criptográfica sobre la cual el propietario de la clave necesite probar su propiedad. **Esta dirección se denomina identificador descentralizado (DID), otro estándar que proviene del W3C**.

Esta es la idea central detrás de pasar de PKI centralizada a PKI descentralizada (DPKI).

3.4 Identificadores descentralizados (DID)

Los identificadores descentralizados son, como su nombre indica, identificadores únicos basados en una PKI descentralizada. Estos identificadores, estandarizados por el W3C, proporcionan un estándar para que los individuos y las organizaciones elaboren identificadores permanentes, únicos y verificables criptográficamente, totalmente bajo el control del propietario de la identidad.

Un DID se puede almacenar en una red blockchain junto con un documento DID que contiene la clave pública para el DID, cualquier otra credencial pública que el propietario de la identidad desee revelar y las direcciones de red para la interacción. El propietario de la identidad controla el documento DID mediante el control de la clave privada asociada.

En este caso el propietario de una entidad ya no depende de un proveedor externo para obtener un identificador único que pueda utilizarse en internet. **Con este modelo cualquier persona puede emitir una credencial firmada digitalmente para que otros pueden verificarla.** Para un

verificador**, solo es necesario tener el DID del emisor** (que podría estar contenido en la misma credencial) **para poder buscar la clave pública del emisor en la red blockchain y verificar la firma en las reclamaciones**.

Cada implementación deberá desarrollar los métodos DID, los cuales serán los mecanismos por el cual un DID y su documento DID asociado se crean, leen, actualizan y desactivan en una red blockchain.

Estos nuevos identificadores están diseñados para permitir que el controlador de un DID demuestre el control sobre él y se implemente independientemente de cualquier registro centralizado, proveedor de identidad o autoridad de certificación. Los DID son una URL (Localizador Uniforme de Recursos) que relacionan un sujeto DID con un documento DID que permite interacciones confiables con ese sujeto. Los documentos DID son documentos simples que describen cómo usar ese DID específico.

3.5 Datos fuera de la red blockchain

En el modelo planteado, solo se almacenará en la blockchain claves públicas que serán accesibles a través de los DID, quedando por fuera de la red toda información privada de la persona dueña de la credencial digital. Por lo cual, de esta forma se define un nuevo concepto que son **los datos que se encuentran fuera de la red** (“datos off-chain”). La necesidad de que cierta información quede fuera de la red blockchain está basada en los requerimientos de cada implementación. Estos casos puedan variar debido a que, por ejemplo, la red blockchain puede tener un límite en la cantidad de datos que se pueden almacenar en un solo bloque, o por el costo de aprobar una transacción a un bloque puede ser muy alto o es necesario compartir información para el cómputo o la verificación, pero los datos en sí son confidenciales o no deberían ser legibles por todas las partes de la cadena.

Esto se vuelve obligatorio cuando una parte quiere verificar cierta información con la cadena de bloques, pero no necesariamente quiere hacer que la misma esté disponible.

O, en algunos casos, se requiere por alguna normativa que los datos sean cambiados o eliminados. Un ejemplo de este caso es el Reglamento General de Protección de Datos (GDPR) en Europa, en donde entre los puntos normados se encuentra el derecho al olvido. Esto quiere decir que una persona puede solicitar que sus datos sean eliminados de cualquier registro. Dicho esto, se plantea el problema frente a una de las características de blockchain que **es la inmutabilidad de los datos, la cual define que cualquier dato almacenado en alguna cadena de la red no puede modificado ni eliminado**. Por lo cual, es necesario almacenar información confidencial fuera de la cadena para que pueda ser eliminada si es necesario. Una solución es cifrar la información en el sistema, para asegurar que, cuando llegue el momento, el "olvido" de las claves garantiza que la información confidencial ya no es accesible.

Otra posibilidad es centrarse en el valor de blockchain para proporcionar evidencia inalterable de hechos escribiendo el hash de las transacciones en él, mientras que las transacciones en sí mismas se almacenan fuera del sistema. Esto mantiene la integridad de las transacciones, al tiempo que permite la capacidad de borrar las transacciones, dejando información restante, "olvidada" en la cadena de bloques.

3.6 Divulgación selectiva de reclamos verificables

La **divulgación selectiva** permite a los propietarios de identidades escoger los datos que se desean compartir en un contexto particular.

El ejemplo clásico es la fecha de nacimiento. Cuando muestra su licencia de conducir en un bar para demostrar que tiene la edad suficiente para beber, el camarero puede ver su fecha de nacimiento completa. No solo es esta información más de lo que realmente necesita saber, sino que también es información que se usa con frecuencia en el robo de identidad.

La divulgación selectiva utiliza una técnica criptográfica conocida como prueba de conocimiento cero (ZKP), de esta forma se puede compartir y verificar información sin revelar datos innecesarios sobre la misma.

El objetivo de este tipo de técnicas **es probar que se conoce algún o varios secretos a alguien, sin que realmente se revele dicho secreto**. En este proceso participan dos partes, el "Probador" del argumento, y el "Verificador" del mismo. La idea básica detrás de esta técnica es probar inequívocamente que el "Probador" conoce el secreto sin revelarlo.

Una técnica recibe el nombre de Prueba de Conocimiento Cero (ZKP), si se cumplen estos tres requisitos:

1. Integridad y exhaustividad: Se asume que las dos partes involucradas (el probador y el verificador) son honestos y seguirán el protocolo. Esto significa que, si un probador da una declaración, el verificador será convencido efectivamente por la misma.
2. Solidez y robustez: El protocolo debe asumir que la honestidad es escasa o nula. Por lo que para probar que efectivamente el probador tiene un secreto, se debe convencer al verificador.
3. Conocimiento cero: Esto significa que si la declaración es verdadera ningún verificador tramposo puede saber más que este hecho. [6]

Entonces en el ejemplo antes planteado, cuando una persona sea poseedora de una credencial digital que represente una licencia de conducir en forma de reclamo verificable, es posible usar una aplicación móvil para demostrar que una persona tiene edad suficiente para comprar una bebida alcohólica (por el límite de edad para obtener la licencia de conducir). El camarero podría verificar la prueba utilizando la clave pública del emisor (similar a la verificación de una firma digital) y en este caso el camarero nunca conoce (es decir, tiene "cero conocimientos de") su fecha de nacimiento real.

3.7 Resumen del modelo

El uso de este tipo identidades hacen posible que los individuos tengan el control total de sus identidades digitales. Las cuales podrán ser validadas por cualquier entidad pública o privada que lo requiera, con autorización del individuo, sin depender de una base de datos central.

Dicho esto, se realizará una síntesis del modelo aquí planteado, nombrado los siguientes aspectos importantes:

3.7.1. Privacidad por defecto y diseño.

El modelo aquí plantado no está definido completamente en una red blockchain, si bien cada DID representa al menos un componente de una identidad digital, solo el propietario de la identidad conoce el "mapa" de qué DID y registros de identidad se encuentran en la red; y cuales reclamaciones y pruebas se han compartido con las partes confiantes fuera de la red. Por lo tanto, la definición definitiva de una identidad digital es información privada del propietario de la identidad.

3.7.2. Se trabajan con DID y claves públicas únicas por pares.

Un DID se almacena en una cadena de bloques junto con un documento DID que contiene la clave pública para el DID, cualquier otra credencial pública que el propietario de la identidad desee revelar y las direcciones de red para la interacción. El propietario de la identidad controla el documento DID mediante el control de la clave privada asociada.

Estos identificadores son únicos y verificables, ya que al crearse se les asocia un par de claves privado-público, en donde la privada es almacenada por el propietario de la identidad (llamada también clave de firma) y la pública en la red blockchain (llamada también clave de verificación).

3.7.3. Reclamos verificables

Los reclamos, son afirmaciones o certificaciones hechas por un individuo sobre sí mismo u otra persona. Los reclamos se firman digitalmente para que cualquier persona/entidad que reciba el reclamo pueda saber quién lo emitió.

Los reclamos poseen una referencia a su definición para que cualquier entidad pueda buscarla y trabajar con ella. Además, poseen claves para cada reclamo las cuales serán utilizadas por cualquier entidad para validar que la reclamación es legítima. Es decir, que las claves de los reclamos están vinculadas al emisor. Es posible cambiar la clave de reclamación, quedando un registro de las claves antiguas, dando la posibilidad a que las reclamaciones puedan caducar o ser revocadas cuando sea necesario.

3.7.4. Divulgación selectiva por defecto. Los reclamos verificables utilizan pruebas criptográficas de conocimiento cero.

Las pruebas de divulgación permiten utilizar las reclamaciones sin revelar información innecesaria sobre el tema. El titular de una identidad puede combinar múltiples credenciales verificables de múltiples emisores en una sola presentación sin revelar credenciales o identificadores de sujeto al verificador.

3.7.5. Verificación

Debido a que cada DID tiene un par de claves público-privadas asociadas, cualquier persona con un DID debe poder emitir digitalmente y firmar reclamaciones verificables y otros documentos. Mientras el verificador tenga el DID del emisor (que se encuentra contenido en la credencial), es una cuestión simple buscar la clave pública del emisor en el blockchain y verificar la firma en las reclamaciones.

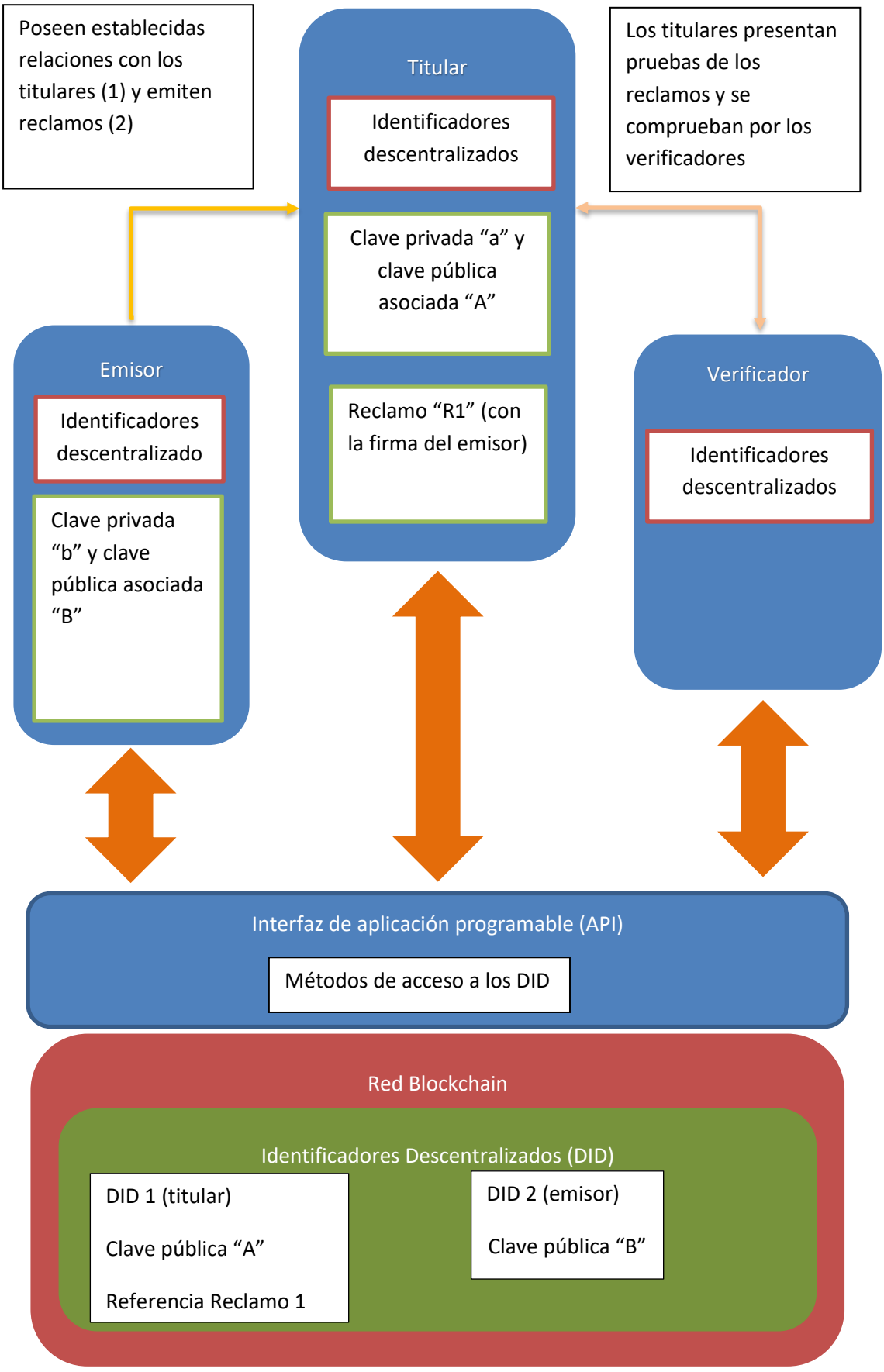

Imagen 5. Resumen del modelo. (desarrollo propio).

(1) Por ejemplo, si una persona posee una cuenta bancaria, existe una relación con su banco. Aquí se crea un DID con sus claves asociadas. La persona comparte su clave de verificación (publica) con el banco, la que creó específicamente para esta relación. Esta clave representa la identidad de la persona con el banco y se puede usar para verificar cualquier interacción que tengan.

El banco también posee su par de claves. La clave pública es almacenada en la red blockchain y es la que representa al banco en la red. Las claves de verificación de la persona y el banco se encuentran en la red, por lo que ambos pueden saber que están utilizando las últimas claves de verificación de la otra parte.

A medida que se agreguen nuevas relaciones, la persona utilizará un par de claves único para cada una de sus relaciones.

(2) La persona posee reclamos, los cuales están firmados digitalmente para poder verificar que entidad los emitió.

Ligeramente basado en el White paper de la firma Sovrin. [4]

4. CONCLUSIONES

En mi opinión, considero que la gestión de identidades digitales es uno de los problemas más antiguos y difíciles en el mundo de internet. Pienso que todavía no hay manera definida, segura y universalmente adoptada en el uso de las credenciales digitales para probar nuestra identidad en línea del mismo modo que lo hacemos en el mundo real. Además, cada persona necesita una identidad digital descentralizada que posea y controle, respaldada por sus propios identificadores que permitan interacciones seguras y confidenciales.

El modelo de gestión de identidades aquí planteado se basa en una billetera digital que sirve como depósito para todo tipo de datos personales y financieros, información que solo se puede compartir después de una solicitud específica y solo con el permiso del propietario (al poseer un par de claves asociadas). Para el desarrollo del mismo, se tuvieron en cuenta las implementaciones ya existentes y, además, se explotaron las características de seguridad que nos brindan los diferentes sistemas y/o protocolos aquí mencionados, para obtener con esto el modelo final.

Este modelo no solo eliminará la dependencia de los registros centralizados para la identidad digital, sino también de las autoridades de certificación centralizadas para la administración de claves, como es típico de la PKI jerárquica (infraestructura de claves públicas).

Con miras a solucionar esto se utilizarán los identificadores descentralizados (DID) que son un nuevo tipo de identificador para una identidad digital verificable y auto-soberana. Los DID están totalmente bajo el control del usuario, independientemente de cualquier registro centralizado, proveedor de identidad o autoridad de certificación.

Estos identificadores hacen posible la interacción de elementos que están fuera y dentro de la blockchain, característica necesaria para el funcionamiento del modelo. Eliminando la dependencia de los registros centralizados para identificadores, así como de las autoridades de certificación centralizadas para la administración de claves. Como cada DID tiene un par de claves público-privadas asociadas, cualquier persona con un DID debe poder emitir digitalmente y firmar reclamaciones

verificables y otros documentos. Mientras el verificador tenga el DID del emisor, es una cuestión simple buscar la clave pública del emisor en la blockchain y verificar la firma en las reclamaciones.

Dentro del análisis realizado sobre las diferentes implementaciones, se pudo constatar que algunas organizaciones, como W3C o Sovrin Foundation, están trabajando en diferentes aspectos de la identidad soberana, generando una gran cantidad de protocolos que han sido publicados de forma abierta. El nivel más alto de los estándares que se están detallando corresponde a las *credenciales verificables,* mediante las cuales se intenta especificar cómo se deberían crear, intercambiar, eliminar y verificar credenciales en el mundo virtual. Podemos mencionar que el paradigma aquí diseñado plantea una solución integral que pone el foco en devolver la titularidad y control de los datos, y por consecuencia de la identidad, a los usuarios, al mismo tiempo les permite la plena libertad para elegir con qué institución entablar una relación, pudiendo llevarse consigo los datos y seguir operando de forma fluida y sin interrupciones mayores.

Con este nuevo concepto, el ciudadano es soberano de su identidad y decide qué información quiere compartir y con quién, pudiendo asociar infinidad de atributos que podrán consumir diferentes organizaciones públicas y privadas. Este proceso, por ejemplo, ya es posible hoy en el mundo de las telecomunicaciones en Argentina, gracias a la portabilidad numérica; la propuesta aquí planteada trae y adapta esta realidad al mundo financiero para resolver como se conoce al cliente.

A lo largo de la tesis se plantearon diferentes objetivos los cuales estaban dirigidos a definir un nuevo modelo de gestión de identidades digitales superador a otras alternativas que existen hoy en el mercado argentino, basándose en las diferentes soluciones que prexisten en el mundo. Poniéndolo, por ejemplo, en una posición de igual frente a las entidades financieras, en un ambiente donde el usuario no confía en lo que hacen dichas entidades con sus datos y al mismo tiempo estas tampoco confían entre sí. Y no solo ello, dado que la propuesta es de carácter abierto, todo tercero interesado puede sumarse y ofrecer servicios relacionados con esta solución

de “credencial financiera”, abriendo el juego a nuevos participantes y efectivizando el principio de banca abierta.

5. BIBLIOGRAFÍA

[1] Identidad Digital: El nuevo usuario en el mundo digital, Fundación Telefónica, http://boletines.prisadigital.com/identidad_digital.pdf (consultada el 02/3/2019).

[2] Modelo de datos de credenciales verificables 1.0. Expresar información verificable en la Web, https://www.w3.org/TR/vc-data-model/ (consultada el 20/3/2019).

[3] Identificadores descentralizados (DIDs) v0.13. Modelo de dato y sintaxis, https://w3c-ccg.github.io/did-spec/ (consultada el 20/4/2019).

[4] Sovrin: un protocolo y token para la identidad soberana y la confianza descentralizada, https://www.sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (consultada el 17/12/2018).

[5] NISTIR 8202: Blockchain Technology Overview, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf (consultada el 14/05/2019).

[6] Qué es Zero Knowledge Protocol (ZKP), https://academy.bit2me.com/zkp-zero-knowledge-protocol/, (consultada el 27/12/2019).