Blockchain vs. Firma electrónica en sector público

Tomás García-Merás Capote

clawgrip@hotmail.com +34 619980058

Contenido

1. Tecnologías base de la confianza de Blockchain

Es importante, antes de entrar en los fundamentos de la confianza en Blockchain y sus fortalezas y debilidades, conocer bien dos de las tecnologías que sobre las que se asienta su seguridad, las huellas digitales y la criptografía asimétrica

1.1. Las huellas digitales

1.1.1. Concepto de huella digital

La huella digital (en inglés "hash" o "digest") es la tecnología que permite comprobar la integridad de cualquier conjunto de datos digitales sin necesidad de guardar una copia del original en sí, entendiendo conjunto de datos digitales como cualquier dato binario, desde una imagen a un documento de texto (Word, PDF, TXT, etc.), pasando por cualquier otro tipo de datos que podamos imaginar: Hojas de cálculo, videos, etc.

El concepto básico es que, a cada conjunto de datos, sin importar su tipo o longitud (tamaño), se le corresponde un número de control de una longitud determinada, normalmente comprendida entre 256 y 512 bits (un tamaño muy reducido y manejable). Si se produjese cualquier cambio, por mínimo que sea, la huella cambiará por completo.

Veamos un ejemplo usando el algoritmo SHA-1 de generación de huellas digitales (se detallarán más adelante qué algoritmos existen para generar huellas digitales):

Del texto (codificado digitalmente en UTF-8): `Universidad de Murcia`

Se obtiene la huella SHA-1:
`6d5279a62132abb8214a8a650506cddfc255b078`

Ahora, si introducimos una pequeña variación, por ejemplo, poniendo una D mayúscula: `Universidad De Murcia`

Se obtiene una huella SHA-1 completamente distinta:
`4f4d0152799fd385607a9da6fe7c68aa2692304f`

Así, conservando únicamente el valor de la huella del texto original, podemos detectar posteriormente alteraciones en este, ya que cualquier texto que se nos presente en el futuro como idéntico al original deberá generar exactamente esta huella, mientras que si fue alterado generaría una huella completamente distinta.

Las huellas digitales se usan comúnmente para el control de la integridad de los datos, limitado este control a la detección de errores en las transcripciones, como puede ser la letra en los números de DNI o los dígitos de control en un número de cuenta bancaria, pero cuando necesitamos que estas huellas añadan seguridad jurídica en lo relativo a la integridad de los datos, el algoritmo debe cumplir dos premisas fundamentales:

1. No debe ser posible, a partir de una huella digital dada, crear un binario arbitrario que genere dicha huella.

La fórmula matemática de generación de huellas debe funcionar únicamente en un sentido: A partir de los datos es posible calcular una huella, pero a partir de una huella no debe ser posible generar un conjunto de datos correspondiente.

2. Debe ser probabilísticamente imposible (extremadamente poco probable) encontrar dos conjuntos de datos distintos que generen la misma huella digital.

Estadísticamente, es efectivamente posible encontrar dos binarios con la misma huella, ya que, poniendo como ejemplo un algoritmo que genere huellas de 256 bits de

longitud, tendríamos 2^{256} huellas distintas, mientras que las combinaciones de datos binarios (sin limitación de tamaño) son infinitas, pero 2^{256} es un número tan elevado de huellas distintas que esta posibilidad es despreciable.

La posibilidad de encontrar dos binarios diferentes con la misma huella (lo que se denomina *colisión*) no depende solo de la longitud de esta, sino también de la uniformidad en la distribución de huellas generadas. Es decir, que evite que haya huellas con más probabilidad de aparecer que otras.

1.1.2. Algoritmos de generación de huellas digitales

El algoritmo de generación de huellas digitales, entendido como la fórmula matemática que extrae la propia huella a partir de la representación binaria de los datos, es distinto según el formato de huella digital que usemos, y existen distintos algoritmos de huella digital:

- Algoritmos obsoletos: MD2, MD5, SHA-1.
- Algoritmos actualmente en uso y considerados como seguros:
    - SHA-2: Secure Hash Algorithm 2: https://es.wikipedia.org/wiki/SHA-2
        - Define una familia de formatos según la longitud de la huella generada: SHA-224, SHA-256, SHA-384 y SHA-256.
            - Tanto el Esquema Nacional de Seguridad (ENS) como el Esquema Nacional de Interoperabilidad (ENI) recomiendan el uso de SHA-256, por ser el que mejor balancea su seguridad con la dificultad que entraña su cálculo y el tamaño en bits que ocupa.
- Algoritmos nuevos que se plantean como opción de futuro por su mejor seguridad:
    - SHA-3: Secure Hash Algorithm 3: https://es.wikipedia.org/wiki/SHA-3
        - Define una familia de formatos según la longitud de la huella generada y ligeras variaciones en su fórmula matemática: SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 y SHAKE256.

Obsolescencia e inseguridad de los algoritmos de huella digital

En la enumeración anterior hemos clasificado ciertos algoritmos como obsoletos, pero ¿cómo pasa un algoritmo a ser considerado inseguro y por lo tanto obsoleto? La principal causa es la reversibilidad de la fórmula de cálculo debido al incremento de la potencia de computo de los ordenadores con el paso de los años.

Las fórmulas de cálculo de huella digital no son completa y absolutamente irreversibles. Es decir, no es completa y absolutamente imposible generar un binario correspondiente a partir solo de la huella digital, sino que se considera que es lo suficientemente costoso computacionalmente como para que no sea viable.

Así, por ejemplo, si incluso juntando una enorme cantidad de computadoras de gran potencia que aunasen sus capacidades de cálculo se tardase más de 50 años en revertir una fórmula de cálculo, podríamos considerar el algoritmo como seguro.

Pero la potencia de cálculo de los ordenadores no permanece constante con el paso del tiempo, cada vez contamos con procesadores más potentes (con lo que la potencia de cálculo se hace más accesible), tal y como expresó Gordon E. Moore (cofundador de la empresa de semiconductores Intel) en su famosa Ley de Moore. Esta ley expresa que

aproximadamente cada dos años se duplica el número de transistores de un microprocesador, lo que implica en la práctica duplicar la potencia de cómputo de este.

Así, la Ley de Moore junto a las mejoras tecnológicas que también se producen en la eficiencia de las tecnologías que permiten combinar las potencias de cálculo de ordenadores distintos, incluso deparados geográficamente y conectados únicamente por redes de comunicaciones, hacen que la perspectiva de 50 años de cómputo que poníamos como ejemplo de seguridad, bajen drásticamente con el paso de los años hasta periodos que sí podemos considerar como inseguros.

1.2. La criptografía asimétrica

1.2.1 Concepto de claves asimétricas

El segundo concepto técnico de importancia que necesitamos conocer para ahondar en los modelos de confianza digital es la criptografía asimétrica.

Este modelo introduce un concepto sencillo en su entendimiento, pero ciertamente complejo en su implementación matemática: Dos claves para el cifrado (encriptado) de datos:

Se tienen siempre dos claves (que se generan conjuntamente según un algoritmo). Lo que se cifra con la primera solo puede ser descifrado con la segunda y al revés (las claves son intercambiables), lo que se cifra con la segunda solo puede ser descifrado con la primera.

En contraposición, la llamada clave simétrica o clave única, usa una sola clave que vale tanto para cifrar como para descifrar.

En los modelos de claves asimétricas, el usuario de estas se reserva una bajo su exclusivo conocimiento y control (que pasa a denominarse clave privada) y distribuye la otra de forma abierta (que pasa a denominarse clave pública).

La utilidad más directa que podemos encontrar en este modelo de claves pública y privada es el cifrado de datos. Si alguien quiere enviarme datos cifrados de forma que solo yo pueda descifrarlos (garantizando su confidencialidad), solo tiene que cifrarlos con mi clave pública, ya que de esta manera solo yo podre descifrarlos, porque soy el único que tiene la clave privada (está bajo mi exclusivo conocimiento y control).

Dentro de que este uso resuelve serios problemas en el mundo del cifrado de las comunicaciones (principalmente el problema que se da en los modelos de clave única de cómo hacer llegar al emisor la clave compartida de forma segura y que este la custodie adecuadamente), hay una segunda utilidad de las claves asimétricas de igual o incluso mayor importancia: Demostrar la autoría de una operación de cifrado.

Si yo cifro un dato con mi clave privada, solo yo he podido hacerlo, puesto que solo yo conozco y tengo acceso a esta clave privada, pero todo el mundo puede comprobar la autoría de este acto de cifrado, puesto que la clave de descifrado (la clave pública), que será la única que pueda descifrar el dato, está públicamente disponible.

1.2.2. Algoritmos de criptografía asimétrica

Al igual que con las huellas digitales, hay diferentes fórmulas matemáticas que pueden aplicarse en los modelos de criptografía asimétrica:

- Algoritmos en desuso:
    - DSA: Digital Signature Algorithm: https://es.wikipedia.org/wiki/DSA

- Algoritmos actualmente en uso:
    - RSA: Rivest, Shamir y Adleman (creadores del algoritmo): https://es.wikipedia.org/wiki/RSA
        - Es el recomendado por el Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad).
- Algoritmos nuevos:
    - ECDSA: Elliptic Curve Digital Signature Algorithm: https://es.wikipedia.org/wiki/ECDSA
        - Es el usado por Blockchain

Obsolescencia e inseguridad de los algoritmos de criptografía asimétrica

Como en prácticamente cualquier área relacionada con la informática, la seguridad absoluta no existe, por lo que, de nuevo, tenemos que hablar de la obsolescencia e inseguridad en los algoritmos.

En el caso de la criptografía asimétrica, tenemos dos aspectos principales que tener en cuenta:

I. Posibilidad de descifrar unos datos sin conocer la clave pública ni la privada.
    a. Normalmente, este tipo de ataques se realizan por "fuerza bruta". Es decir, probando todas y cada una de las posibles combinaciones de una clave. El éxito de este ataque depende de:
        i. Longitud de la clave. Una clave de 512 bits de longitud nos da 2^{512} combinaciones posibles, mientras que una de 2048 nos ofrece 2^{2048}, una cantidad tremendamente mayor.
        ii. Cuantas combinaciones puedo probar por unidad de tiempo. Esto depende directamente de la potencia de proceso de los computadores.
            1. Como comentábamos anteriormente, por la Ley de Moore, esta capacidad se duplica cada dos años.
II. Posibilidad de, teniendo la clave pública, inferir la privada.
    a. Hay diferentes parámetros en los algoritmos de generación de pares de claves (especialmente la generación de números aleatorios) que pueden propiciar esta posibilidad.
        i. Por ejemplo, un error en la generación de números aleatorios en ciertos procesadores de la empresa Infineon (usados en tarjetas inteligentes) ha hecho que muchos DNIe expedidos se hayan tenido que revocar (en lo referente a sus claves internas) por inseguros, al poderse inferir (al menos teóricamente) la clave privada a partir de la pública.
            1. Vulnerabilidad ROCA (CVE-2017-15361): https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-15361

1.3. Firma electrónica

Teniendo ya asentados los conceptos de huella digital y de criptografía asimétrica, llegamos por fin a la base de la confianza en Blockchain (y en otros muchos modelos de confianza): La firma electrónica.

El proceso es sencillo, imaginemos para describirlo que tenemos un documento a firmar en formato electrónico, que puede ser cualquier binario, desde un documento Word o

PDF hasta una imagen PNG o JPEG… Sobre este conjunto de datos, calculamos su huella digital y ciframos esta con nuestra clave privada.

¿Qué resultado hemos obtenido? Gracias a la huella electrónica, un resultado vinculado unívocamente a un único documento, que no puede ser alterado ni modificado de forma posterior a la firma (ya que la huella dejaría de coincidir), y gracias a las claves asimétricas, un resultado que solo yo he podido generar (como única persona que tiene esta clave privada), aspecto comprobable por todo aquel que tenga mi clave pública.

En suma: Una firma electrónica de un documento.

2. La confianza en Blockchain

2.1. Identidad

Uno de los pilares de cualquier modelo de confianza es la identidad. En la gran mayoría los sistemas transaccionales electrónicos, para cualquier sector, necesitaremos conocer a los autores de las transacciones, a los poseedores de los activos y a los firmantes de los documentos.

Como hemos comentado anteriormente, la identidad en un sistema de criptografía asimétrica como es Blockchain, se basa en la tenencia de la clave privada.

Sobre esta tenencia, podemos definir, a grandes rasgos, dos modelos de identidad:

- Sin identidad: La clave privada como un título al portador.
    - Es el modelo usado en la mayoría de las criptomonedas, como Bitcoin. El poseedor de la clave privada es el poseedor de los activos asociados, pero no hay ningún tipo de identidad, por lo que no es posible afirmar que el actual poseedor de una clave privada haya sido el autor de transacciones pasadas firmadas con esta clave.
    - Evidentemente, no es posible montar sistemas de confianza sobre este modelo relacionadas con la identidad de las partes.
- Identidad delegada en los integrantes de la red.
    - La identidad va ligada a la posesión de la clave privada, y esta tiene una correspondencia con un ente real (una persona, una entidad, una máquina…) que se determina por un consenso entre los participantes de la red sustentado sobre testimonios firmados.
    - Además de la mera identidad (“quién soy”), la red también puede determinar las capacidades del sujeto (“qué soy capaz de hacer”).
- Identidad respalda por autoridades de certificación.
    - Una combinación de autoridades (Autoridad de Registro, Autoridad de Certificación y Autoridad de Validación) asocia una clave pública (y por tanto su correspondiente privada) a una persona concreta.
    - Se establecen formalmente una serie de condiciones de uso de las claves: Prácticas y políticas de certificación, perfiles de certificados, términos y condiciones, etc.
    - Tienen un respaldo legal nacional (Ley 59/2003) y europeo (reglamente eIDAS). Su validez legal es paneuropea.

2.1.1. Identidad por consenso en la red

Como hemos avanzado en el punto anterior, un posible modelo de identidad, que encaja perfectamente en la arquitectura de Blockchain, es el basado en los consensos de los miembros de nuestra red.

En este modelo, los miembros de una misma red transaccional se asignan las identidades entre sí, junto a las capacidades asociadas a estas identidades mediante un modelo de consenso, de igual forma que en Blockchain se dan por buenas las transacciones.

En una simplificación y según este modelo, yo soy Tomás García-Merás porque la gran mayoría de la red reconoce que es así (asociando esta identidad a mi clave privada) y, de igual manera, Tomás García-Merás es capaz de, por ejemplo, programar en Java porque, de nuevo, los integrantes de la red le reconocen mayoritariamente esta capacidad.

Un ejemplo de implantación de este modelo de identidad es la red Blockchain Alastria (https://alastria.io/), en el llamado Alastria ID.

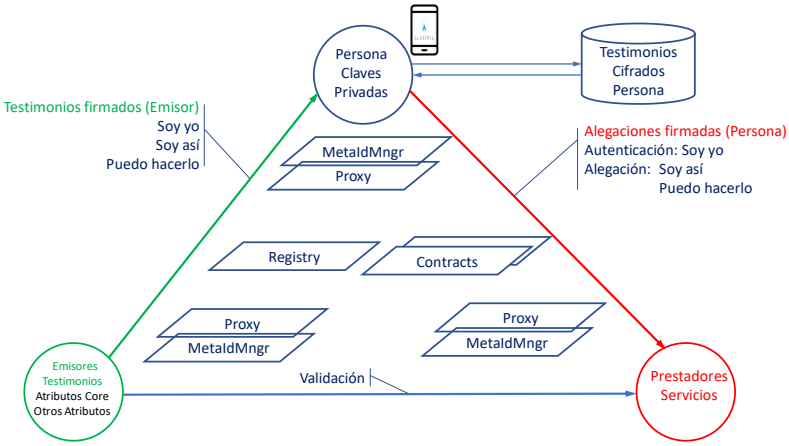

Ilustración 3: Alastria ID. Fuente: Alastria

En Alastria ID, las identidades se definen en las llamadas alegaciones de identidad. Una alegación de identidad es poco más que una colección de testimonios firmados por sus emisores (miembros de la red).

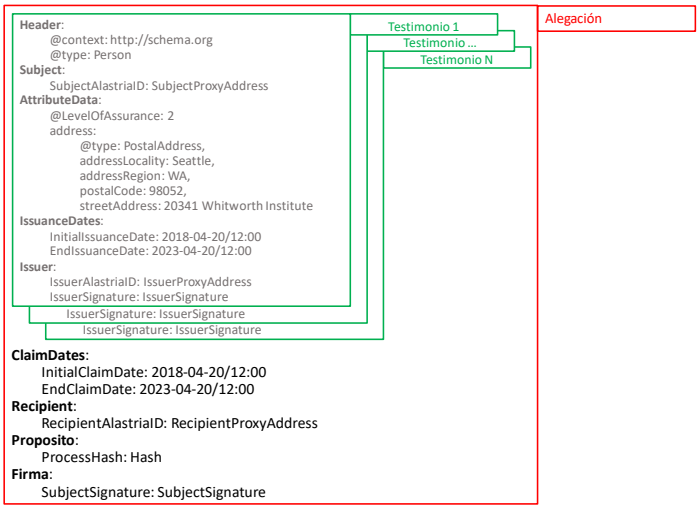

Ilustración 4: Alegaciones de identidad en Alastria ID. Fuente: Alastria

Estas alegaciones van enlazadas con las transacciones mediante una clave pública (que siempre estará vinculada a una privada).

La confianza de estos modelos de identidad basadas en consenso se basa principalmente igualmente en el consenso en su reconocimiento por los integrantes de la red. Si todos

los integrantes de una red acuerdas respetar y reconocer los consensos sobre identidad que se formen dentro de la misma red.

La principal ventaja de este modelo es la independencia. La red es autosuficiente para proporcionar o retirar identidades. Esto es especialmente importante en una red Blockchain, ya que, si la confianza reside en la red de forma completamente interna, se eliminan las dependencias externas que requerirían la intervención de Oráculos o delegaciones de confianza.

Las desventajas vienen por dos lados:

Por una parte, el proceso de incorporación de nuevos miembros nominados (con identidad) a la red no es inmediato. El nuevo miembro debe hacerse conocer por toda la red para conseguir el consenso necesario para el reconocimiento de su identidad, y este proceso puede ser lento, complejo o consumir demasiados recursos.

Por otra, tenemos el inconveniente de que una identidad reconocida en la red puede tener dificultades en ser reconocida fuera de esta, y dado que las redes como Blockchain no operan completamente aisladas, tarde o temprano necesitarán este reconocimiento externo, ante, por ejemplo, auditores, autoridades judiciales, autoridades tributarias u otras autoridades del sector público.

2.1.2. Identidad respaldada por autoridades

Otro modelo de identidad que podemos aplicar a las redes como Blockchain es la basada en autoridades. Aquí, es una autoridad externa a la red la que vincula una clave a una identidad y asegura su validez.

Siguiendo la simplificación que desarrollábamos anteriormente, yo soy Tomás García-Merás porque así lo asegura el Cuerpo Nacional de Policía, y así lo ha certificado expidiéndome un Documento Nacional de Identidad (que además contiene mis claves asimétricas). Además, podemos asegurar que sé conducir porque así lo asegura la Dirección General de Tráfico, que lo certifica expidiéndome un permiso de conducir.

Este modelo simplifica enormemente el aseguramiento de la identidad y las capacidades cuando se tienen autoridades en las que todos confían (puede ser tanto dentro como fuera de la red). Ya no tengo que convencer a una mayoría de los miembros de mi red de qué sé conducir, únicamente a uno (DGT), que se cerciora de ello por sus propios medios (en este caso, mediante un examen teórico y otro práctico).

La gran ventaja de este modelo es que estas autoridades pueden estar respaldadas legalmente, lo que le otorga una validez jurídica: Una identidad certificada mediante un pasaporte es reconocida en prácticamente todo el mundo, un título universitario español es reconocido por todos los estados miembros de la Unión Europea, etc.

Para los casos normales de identidad basada en claves asimétrica, se establece normalmente el siguiente modelo:

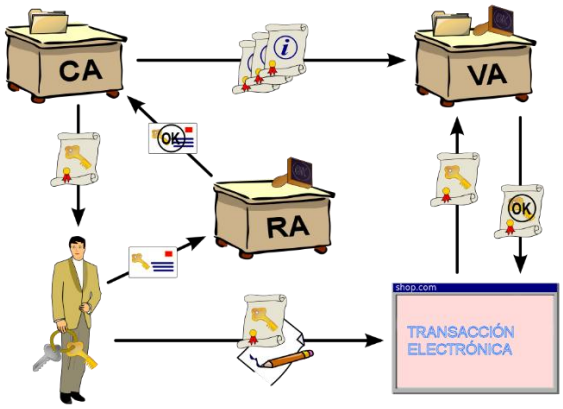

Ilustración 6: Modelo de identidad basado en autoridades. Fuente: Wikipedia

I. El usuario genera un par de claves, una privada y una pública.
    a. La privada la mantiene siempre privada, bajo su exclusivo control, siendo intransferible.
II. El usuario acude a una Autoridad de Registro (RA) con su clave pública (jamás expone la privada). La RA comprueba (por los medios que determine como apropiados) la identidad del usuario, e informa a la Autoridad de Certificación (CA) que esa clave pública pertenece a ese usuario, que ha identificado.
    a. También puede determinar una capacidad específica del usuario. Por ejemplo, ser empleado de una empresa, ser apoderado de firma o administrador de una corporación, etc.
III. La Autoridad de Certificación (CA) expide un certificado firmado en el que asocia al usuario identificado con la clave pública.
    a. El certificado se le entrega al usuario, pero también se hace público para que todo el mundo pueda conocer la relación entre usuario y clave pública.
IV. El usuario opera con su certificado y su clave privada (que nunca sale de su control).
V. Los participantes en una transacción (o los simples observadores o auditores) pueden acudir a una Autoridad de Validación (VA) para consultar si un certificado es válido:
    a. Está dentro de su periodo de validez.
        i. Los certificados tienen un periodo de validez (inicio y fin), lo que obliga al titular a renovar su demostración de identidad y capacidades y protege contra la obsolescencia (en la renovación pueden usarse tecnologías más modernas y seguras).
    b. No ha sido revocado. Un certificado puede revocarse por distintos motivos.
        i. El titular ha fallado en la custodia de la clave privada y no puede asegurar que no haya caído en otras manos (por ejemplo, ha perdido el DNIe con el PIN apuntado en la propia tarjeta).
        ii. Ha perdido unas de las capacidades que acreditaba el certificado (por ejemplo, ha dejado de ser empleado de la empresa).
        iii. Ha sido descubierta una vulnerabilidad tecnológica que no permite seguir respaldando la seguridad del certificado emitido.
        iv. Etc.
    c. Es correcto e íntegro.

i. Está adecuadamente firmado por la CA, etc.

Este modelo surgió como parte del respaldo legal a la firma electrónica reconocida según la Ley 59/2003 y fue la base de la modernización del sector público según la Ley 11/2007 (tareas que continúan con las leyes 39 y 40 de 2015), por lo que podemos afirmar sin miedo que son esquemas estables y bien asentados jurídicamente, de los cuales contamos ya con jurisprudencia.

Adicionalmente, y en una serie de acciones culminadas con la aprobación del reglamento eIDAS (UE N.º 910/2014) tenemos todo un esquema de autoridades que son reconocidas por todos los estados miembros (la Unión Europea publica una lista, llamada TSL, con todas las autoridades de certificación con reconocimiento paneuropeo: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers), lo que facilita la confianza internacional con respaldo jurídico.

Por último, una ventaja adicional nada desdeñable de la identidad basada en autoridades es que podemos ligar las transacciones a los usuarios y no a las claves de este. Si, por ejemplo, en Bitcoin la pérdida de la clave privada supone la pérdida de todos los fondos asociados, las firmas electrónicas hechas con DNIe siguen siendo válidas (incluyendo en su titularidad) aunque perdamos el DNI (que contiene la única copia de la clave privada). Una renovación del DNIe nos dará una tarjeta nueva con unas claves distintas, pero no supone ningún problema, porque todas las transacciones están asociadas a la persona por su número de DNI (que no varía y es intransferible), y no a las claves.

2.2. No repudio

El concepto de no repudio va ligado íntimamente al de identidad. Básicamente, consiste en la posibilidad de negar la autoría de una transacción firmada electrónicamente. Esta firma no tiene por qué ser una firma electrónica clásica, sino que puede extenderse el concepto a una operación con clave privada sobre la cadena de bloques de Blockchain (como detallamos con anterioridad al repasar las tecnologías base de la confianza).

El repudio puede, por supuesto venir de cualquiera de las partes. Yo puedo negar haber hecho una transacción u operación o alguien puede poner en duda que haya sido yo el que la haya hecho.

Evidentemente, en un marco de anonimato (como, por ejemplo, Bitcoin), no existe ese concepto, pero en las redes con sistemas de identidad si, y es nuestro segundo pilar de la confianza, ya que, si no podemos limitar la capacidad de repudio, en caso de un conflicto tendremos un serio problema.

2.2.1. No repudio en identidad por consenso

En los modelos de identidad por consenso, el no repudio se sustenta en la acumulación de evidencias. No podemos asegurar a priori si un usuario identificado fue realmente el que hizo o no la operación, teniéndolo que determinar a posteriori examinando las pruebas que podamos encontrar (entre las que figurarán los testimonios de identidad).

El problema recae en la incertidumbre en la determinación de suficiencia de esas evidencias en caso de un conflicto, ya que normalmente su evaluación se realizará de forma externa a la red (juez, mediador, etc.) y evaluando también evidencias externas.

2.2.2. No repudio en identidad respaldada por autoridades

En el caso de la identidad basada en autoridades, cuando estas autoridades están reconocidas, el no repudio está garantizado legalmente. Esto significa que una operación hecha con una clave privada asociada a un certificado reconocido es válida a

menos que se demuestre lo contario. La carga de la prueba se ha invertido, ante la ausencia de evidencias, no se puede negar la autoría, en contraposición a otros modelos de identidad, donde, en ausencia de evidencias a favor, legalmente se decide en contra.

Dispositivos Seguros o Cualificados de Creación de Firmas

Una de las bases para no permitir repudio cuando se usan modelos de identidad respaldados por autoridades es el uso de Dispositivos Seguros o Cualificados de Creación de Firmas (SSCD, *Secure Signature Creation Device*). Este tipo de dispositivos realizan una custodia de la clave privada de tal fortaleza que es posible afirmar con seguridad que no hay copias ni usos no autorizados de estas:

- Las claves se generan dentro del SSCD y no es posible extraerlas de ninguna manera, de forma que no es posible que exista una copia fuera del SSCD.
- Las claves se usan dentro del SSCD, nunca salen de este, ni en el momento de ser usadas.
    - El SSCD recibe una huella digital, y hace el cifrado asimétrico en su interior, devolviendo el resultado.
- El uso del SSCD está bajo el exclusivo control del propietario de las claves.
    - PIN, contraseñas, claves de un solo uso (OTP), bloqueos en caso de fallo en la identificación, etc.

En un principio (Ley 59/2003), los SSCD estaban limitados a dispositivos hardware que custodiaba personalmente el titular (como el DNIe), pero el reglamento eIDAS introdujo la posibilidad de que fuese un tercero el que custodiase las claves, como el CNP en el caso de Cl@ve Firma (http://clave.gob.es/clave_Home/dnin.html) o la FNMT en los sistemas de firma en la nube para empleado público, habilitando así modelos en la nube.

2.3. Longevidad de las referencias externas a la cadena de bloques

Cuando queremos referenciar a un activo digital (por ejemplo, el clausulado de un contrato en formato PDF) en una transacción registrada en la cadena de bloques, lo usual es no incluir el propio activo en el bloque, sino usar su huella digital (de mucho menor tamaño). Como la huella digital referencia unívocamente a un activo, son plenamente equivalencias, y se gana en eficiencia y economía de proceso en Blockchain.

No obstante, muchas transacciones pueden requerir que su seguridad jurídica se prolongue por mucho tiempo (pensemos por ejemplo en un contrato hipotecario, con duraciones de hasta 40 años) ¿Qué pasa entonces cuando el algoritmo de huella digital se vuelve obsoleto y vulnerable? ¿Se pierde la confianza en las transacciones antiguas hechas con él?

Efectivamente, en el momento en que la correspondencia entre activo y huella no es unívoca, y podemos tener dos activos con la misma huella, no es posible asegurar a cuál de ellos hace referencia la transacción en la cadena de bloques.

En la firma electrónica avanzada, este problema se resuelve (al menos parcialmente) con el resellado periódico. Cada cierto tiempo (depende de la política declarada) se resellan las huellas digitales, usando el algoritmo y formato más seguro que exista en ese momento. Así, si se realizaron antiguamente firmas usando MD5 o SHA-1, estas estarán reselladas con SHA-2 y, previsiblemente, lo estarán con SHA-3 antes de que SHA-2 se vuelva obsoleto y vulnerable.

En Blockchain la solución pasa por aplicar similares políticas de resellado, si bien no hay políticas públicas de confianza que concreten estos protocolos. Además, el resellado es un serio problema en Blockchain debido al altísimo coste de las transacciones.

2.4. Momento en el que se realizan las transacciones

Jurídicamente, es vital conocer el momento en el que se realizan las transacciones u operaciones en la red. No es lo mismo firmar un seguro de accidentes antes que después de sufrir un accidente, o realizar una venta en un ejercicio fiscal que en otro.

En los modelos tradicionales (como las firmas electrónicas básicas), el momento (fecha y hora) se recoge del equipo del que realiza la transacción en lo que se llama una marca de hora. Por supuesto, a menos que este fuera un hecho aislado, siempre se pueden aportar más evidencias de este momento, como, por ejemplo, los registros en los servidores (que recogen a su vez la hora configurada en ellos).

En las redes Blockchain el caso se simplifica un poco, ya que las evidencias las proporcionan los integrantes de la cadena. Particularmente, en Blockchain, la marca de hora que figura en cada bloque de la cadena la proporciona el minero que completa la transacción, aceptándose, normalmente (valor definido en Ethereum y derivados) un desfase de hasta 900 segundos (15 minutos) respecto al inicio de esta.

Así, podemos afirmar que el momento en el que la red da por buena una transacción (por el consenso implícito en Blockchain derivado del trabajo de minería, normalmente) es el único en el que podemos demostrar la existencia de la transacción en sí y que se apoya en la sincronía de los relojes de los equipos de la red, pero que puede registrarse con un retraso de quince minutos desde que se ordenó.

No obstante, de nuevo tenemos una alternativa basada en autoridades: Los sellos de tiempo emitidos por Autoridades de Sellado de Tiempo (TSA).

El funcionamiento de estas autoridades es tremendamente sencillo: El usuario envía una huella digital a la TSA y esta devuelve esta huella junto con la fecha y hora en la que la ha recibido, todo ello firmado electrónicamente. Esto es una demostración efectiva de que el activo digital existía en ese momento, ya que de otra forma no sería posible conocer su huella. El proceso de sellado se realiza mediante un servicio Web y tarda muy poco tiempo (unos pocos segundos en el peor de los casos).

Por supuesto, podría darse el caso de que el activo digital existiese antes de ser enviado a la TSA, por eso es importante recordar que la TSA certifica la existencia de un activo a partir del momento de la recepción de su huella digital, pero no antes. Es posible definir políticas de firma electrónica que establezcan un desfase máximo entre la marca de hora y el sello de tiempo de unos pocos minutos, para tener cierta coherencia.

La gran ventaja de los sellos de tiempo emitidos por TSA reconocidas es que estos tienen validez legal. Nadie puede argumentar que el servidor o el equipo tenían una fecha mal puesta o que hubo manipulaciones. La ley dará por hecho la existencia del activo en la fecha del sello sin necesidad de aportar evidencias adicionales, y sin aceptar ningún “periodo de gracia” de variabilidad.

3. Implementación en Blockchain de los modelos basados en autoridades

Los modelos basados en autoridades son muy anteriores a la aparición y popularización de Blockchain, y fueron diseñados principalmente para la confianza Web (sitios web seguros con SSL y HTTPS) y la firma electrónica convencional.

Hemos detallado anteriormente que las bases tecnológicas de Blockchain son las mismas que las de la firma electrónica, pero el uso de autoridades en este primero no siempre resulta fácil.

Hay cambios puramente de negocio, como el ligar las transacciones a la identidad real y no a las propias claves, pero también hay requisitos técnicos de importancia.

3.1. Certificados y autoridades de certificación y validación.

El único requisito para el uso de certificados reconocidos para operar en una red Blockchain es que estos sean compatibles tecnológicamente. El requisito fundamental es que las claves sean ECDSA, si bien puede ser también necesario que contengan algunos atributos específicos.

La mayoría de las Autoridades de Certificación (CA) expiden únicamente certificados de tipo RSA, pero cada vez es más común que soporten también ECDSA.

Además de poder usar los certificados, es necesario que todas las partes de la red puedan verificar el estado de un certificado, consultando con una VA.

Ciertos sistemas de Blockchain, como HyperLedger, tienen ya facilidades para la integración de las operaciones de validación contra Autoridades de Validación, pero en otras, como Ethereum, es necesario implementarlo a medida, y dado que las VA no operan dentro de la cadena de bloques, habrá que hacerse mediante oráculos, lo cual resulta complejo.

3.2. Huellas digitales

Las huellas digitales son un aspecto neutro, excepto que tendremos que tener siempre en cuenta que cuando se usen para referenciar activos fuera de la cadena de bloques y necesitemos longevidad en su confianza, deben definirse políticas de resellado, que en Blockchain significarían introducir, en un nuevo bloque, un puntero al bloque anterior junto con la huella del activo calculado con el nuevo algoritmo.

Por supuesto, el uso de los algoritmos más actuales (como SHA-2) ayudará a retrasar la invalidez por obsolescencia de las referencias.

3.3. Sellos de tiempo

En el caso de Blockchain, el uso de TSA y sellos de tiempo es un aspecto puramente de negocio ajeno a la tecnología de Blockchain. Si necesitamos precisión y seguridad jurídica del momento de las transacciones, debemos sellar la información antes de que sea procesada en Blockchain.

4. Un ejemplo de aplicación: Sistema de licitaciones electrónicas

Veamos ahora como podríamos poner en práctica los conceptos anteriormente desarrollados en un hipotético sistema de licitaciones electrónicas.

En este sistema, buscaremos distintos objetivos (relativos a la confianza):

1) Nadie debe conocer el contenido de las ofertas hasta el cierre del plazo de presentación.
2) No se pueden hacer cambios en las ofertas una vez presentadas.

El sistema puede aportar además otras ventajas, como el cálculo automático mediante contratos inteligentes de los aspectos valorables mediante fórmulas, pero son secundarios en lo que respecta a la confianza.

4.1. Confidencialidad de las ofertas

Un caso típico de corrupción es el comunicar, antes del cierre del plazo de la presentación, el contenido de la oferta de una empresa (que ha la ha entregado de forma temprana dentro del plazo) a otra (que espera a tener esta información privilegiada antes de presentar la suya), así que, para evitarlo, plantemos que, durante el plazo de presentación, las empresas no envíen sus ofertas, sino la huella digital de estas. De esta forma, no tendremos su contenido, sino una referencia unívoca e inmutable a él.

Pero… Mejoremos aún más el sistema. Hagamos que se envíen las firmas electrónicas de las ofertas, pero no estas (hay un tipo de firma electrónica, llamada *detached*, que no contiene el propio contenido firmado). Estas firmas contendrán no solo la huella de la oferta, sino también los datos del apoderado que la firma, cumpliendo así dos funciones, por una parte, identificar al remitente, y por otra cumplir la parte de la Ley de Contratos del Sector Público que indica que las ofertas deben presentarse firmadas.

El organismo que recibe las firmas electrónicas *detached* puede aplicarles inmediatamente un sello de tiempo usando una TSA, devolver un recibo firmado a la empresa y… ¿Registrar esta firma en la cadena de bloques? ¡No todavía!

Un aspecto crítico en la confidencialidad es que nadie debe conocer ya no solo el contenido de una oferta, sino incluso que se han presentado ofertas a una licitación. Una empresa podría monitorizar la cadena de bloques observando cierto tipo de actividad en ella, y si durante el plazo de presentación observa actividad, significa que se ha presentado alguien, y si no hay ninguna actividad, significa que no tiene competencia. Esto puede llevar a que los que presenten las ofertas antes estén en situación de desventaja respecto a los que presentan a última hora…

Así, el organismo esperará al cierre del plazo para publicar todas las firmas electrónicas, con su sello de tiempo, en la cadena de bloques. En ese momento todo el mundo podrá conocer quién se ha presentado, pero si quisiésemos esconder ese dato bastaría con insertar solo las huellas de las firmas (equivalente a una doble indirección: Las huellas de las huellas), para que ya no figuren los certificados de los apoderados.

Con este sistema, nadie ha podido tener acceso prematuro a datos de las ofertas, ya que las empresas aún no han enviado su contenido.

La comprobación de los certificados de las firmas de las huellas es un tema bastante más complejo. Podría delegarse en un oráculo, que tendría que llamar a la VA para verificar el estado del certificado, pero igualmente deberían hacerse comprobaciones de que realmente esa persona puede actuar en representación de esa empresa.

Esta última comprobación es sencilla si el apoderado usa un certificado de representación (persona física en representación de persona jurídica), pero si usa un certificado normal, debería hacerse una llamada al CORPME (Registro Mercantil) para asegurarnos. El CORPME dispone de un servicio web de consulta de representantes, que devuelve la adscripción firmada electrónicamente. Por supuesto, otra opción sería

tener un registro previo de empresas que pueden licitar, con las identidades previamente dadas de alta, por lo que podríamos apoyarnos en los datos del certificado (DNI/NIE) para verificarlo contra esta lista (de nuevo los certificados son de gran ayuda).

4.2. Integridad de las ofertas

Una vez publicadas las huellas en la cadena de bloques, las empresas deben publicar el contenido de estas, por lo que debe darse una nueva ventana de tiempo para esta segunda presentación.

Cuando se presentan las ofertas, la comprobación es directa: ¿Coincide la huella digital de la oferta con la de la firma ya insertada en la cadena de bloques? Si no es así es que la oferta se ha modificado, por lo que quedaría invalidada, mientras que si coincide debe darse por válida.

Para el caso de los requisitos evaluables mediante fórmulas, es interesante que las ofertas puedan formalizarse en forma de XML o JSON de muy bajo tamaño (por ejemplo, con los importes ofertados, el número de perfiles propuestos, etc.). Si fuésemos capaces de insertar estas ofertas completas (de ahí la necesidad de un tamaño reducido) en la cadena de bloques tendríamos que cualquier podría comprobar:

- Quién ha presentado la oferta, gracias al certificado de la firma.
- El momento exacto de presentación de la oferta:
    - Está en la cadena de bloques desde antes de la presentación de su contenido.
    - Contiene un sello de tiempo de una TSA.
- Que no se han hecho cambios con posterioridad: La cadena de bloques es inmutable.
    - No puede darse el caso de firmar y sellar varias ofertas, cada una con un contenido, y luego seleccionar la que más convenga conociendo los datos de las otras empresas.
- Evaluar directamente los resultados en el caso de los expedientes que solo contengan apartados evaluables mediante fórmulas.
    - Esta evaluación podría hacerla directamente el contrato inteligente.

5. Conclusiones

La cadena de bloques es una tecnología extremadamente potente que tiene sus raíces en la firma electrónica, pero quedarse en estas raíces con la tecnología (huellas digitales y criptografía asimétrica) y descartar la parte más formal (respaldo de autoridades) puede hacernos perder las grandes ventajas que ofrece combinar ambos mundos.

El ejemplo desarrollado anteriormente, sin certificados digitales reconocidos o sellos de tiempo, pese al uso de Blockchain, tendría importantes carencias en su seguridad, de igual forma que las tienen los sistemas actuales que solo usan firma electrónica.

Nuestro entorno de negocio nunca es un área cerrada sin interacciones externas, siempre tendremos que responder ante autoridades judiciales, regulatorias, fiscales, auditores… Una confianza pactada dentro de este entorno de negocio puede ser suficiente en muchos casos, pero el apoyarnos en autoridades electrónicas reconocidas (CA, RA, VA, TSA, etc.) ampliará estos modelos de confianza y les dotará de seguridad jurídico-legal en toda la Unión Europea, gracias al reglamento eIDAS.