uc3m | Universidad Carlos III de Madrid

BLOCKCHAIN PARA LA MEJORA A NIVEL LOCAL DE LA PARTICIPACIÓN POLÍTICA, DE LA ACTIVIDAD DE LA SOCIEDAD CIVIL Y DE LA ACTIVIDAD ECONÓMICA

Pauline Heit

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement n. 101007820.
This document reflects only the author's view. The Research Executive Agency is not responsible for any use that may be made of the information it contains

Contenido

Abreviaturas:

CNIL	Commission nationale de l'informatique et des libertés
DAPP	Aplicación Descentralizada
DLT	Distributed Ledger Technology o tecnologías de libro mayor distribuido
DPoS	Delegated Proof of Stake o Prueba de Participación Delegada
EBSI	European Blockchain Services Infrastructure
MiCA	Propuesta de Reglamento del parlamento europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937
P2P	Peer-to-peer o red entre pares
PoA	Proof-of-Authority o Prueba de Autoridad
PoS	Proof-of-Stake o Prueba de Participación
PoW	Proof-of-Work o Prueba de Trabajo
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
SA	Sociedad Anónima
SARL	Sociedad de Responsabilidad Limitada
SAS	Sociedad por Acciones Simplificada
UE	Unión Europea

Introducción:

En un momento de crisis de confianza e insatisfacción con los intermediarios tradicionales, instituciones, bancos y estados, la tecnología blockchain, que promete la desintermediación y la transparencia se vuelve muy atractiva.

El término "blockchain" apareció en 2008 con Satoshi Nakamoto y desde entonces hemos visto un crecimiento de los proyectos basados en esta tecnología (De Filippi & Wright, 2019, pág. 28).

Esta tecnología disruptiva revoluciona nuestros sistemas económicos, nuestros sistemas sociales, educativos, digitaliza las Administraciones, reinventa la forma en la que intercambiamos entre sí y mejora la eficiencia de nuestras ciudades, nuestras

administraciones y el uso de los recursos con un objetivo de sostenibilidad y reducción de los costes. El blockchain tiene, por lo tanto, un papel preponderante en la creación y en el desarrollo de las Ciudades Inteligentes y por lo tanto se está imponiendo en todos sus ámbitos ya que su concepto de tecnología distribuida tiene el potencial de transformar los usos.

El blockchain es una tecnología nueva y novedosa, pero el modelo de registros compartidos ya existía hace tiempo. La tecnología blockchain viene a solucionar los defectos que tenían nuestros primeros modelos de redes compartidas y de economía colaborativa volviéndoles mucho más seguros y transparentes para adaptarse a una Sociedad cada vez más escéptica.

Para ilustrar sus principios, volvemos cinco mil años antes de Cristo, en el sur del actual Irak, Sumer es una región de la antigua Mesopotamia donde hubo una doble invención: la primera escritura conocida como escritura cuneiforme y los registros. Los sumerios inventaron un sistema de signos y crearon tablillas de arcilla para contabilizar bienes y transacciones. Así, en su origen un registro compartido tenía una finalidad contable y las tablillas de arcillas son por consecuencia los primeros registros en sí. Los registros son una invención clave de la humanidad, para el comercio, el censo, los catastros, etc. Gravados en arcilla, permitían a los sumerios consultarlas y usarlas todas las veces necesarias y por lo tanto es un sistema pensado para evitar los conflictos entre los habitantes sobre sus bienes. En esta época, pocos son los que sabían escribir por lo cual, este sistema funcionó porque los habitantes tenían confianza en este "tercero de confianza" que son los escribas y luego, porque podían consultar los registros que son inalterables porque gravado en la arcilla.

Ahora como ejemplo de sistema informático distribuido, creado en 1999 Napster es un software de intercambio de archivos de música y videos que es un pionero del modelo Peer-to-Peer, permitiendo que cada cliente se convierte en un servidor pudiendo acceder cada uno a la música que tenga el otro en su biblioteca musical. Los sistemas P2P permiten compartir recursos e información de forma masiva a un coste y escala que serían difíciles de conseguir en un sistema tradicional cliente-servidor. Pero, la popularidad de Napster cayó cuando los tribunales condenaron al gestor del índice de la música disponible, es decir, al que actuaba como eje de la red por infracción de derechos de autores. (De Filippi & Wright, 2019, pág. 25)

Así, el blockchain tiene un funcionamiento parecido a los dos ejemplos más arriba, pero la clave de su funcionamiento está en que los registros alojados en la cadena de bloques no son creados ni implementados por una sola persona en la que tendríamos que confiar sino en una multitud de personas que juntas garantizan la veracidad de los registros. Es así más fácil confiar en un registro distribuido, abierto, tiene tantas copias que tiene de nodos en el blockchain, las informaciones antes de inscribirse son autentificadas por todas las personas que tienen un papel en el blockchain (los nodos) y sobre todo la clave está en su vocación de ser transparente por lo cual la información alojada en el blockchain puede ser consultada según el tipo de blockchain elegido. Aunque no sabemos leer el lenguaje informático y las informaciones encriptadas en el blockchain igual que los sumerios y su lenguaje cuneiforme, no es un problema porque la clave está en la confianza que tenemos en esta tecnología y en los "terceros de confianza" que certifican que la información registrada en el Blockchain es veraz.

Entonces, el Blockchain es una base de datos descentralizada por lo cual no hay un servidor central ni un gobierno, sino una red formada por todos los usuarios de esta cadena de bloques, llamados "nodos" (ordenadores). El otro aspecto novedoso es que permite realizar transacciones seguras y transparentes entre pares (P2P) por lo cual no necesitamos confiar en una sola persona o entidad designada, sino que confiamos en una multitud de personas. Así desaparecen los intermediarios tradicionales que hubiéramos necesitado en el pasado para realizar una transacción, como los bancos, agencias, empresas. (Guillard, 2020)

Ahora bien, puede ser a la vez una amenaza o una oportunidad dependiendo de la intención de sus creadores. El lado peligroso reside en que todavía no existe un marco jurídico uniforme en Europa que rige el Blockchain ni tampoco existe "nacional" uno en todos los países del espacio comunitario. (De Filippi & Wright, 2019, pág. 195) El riesgo es que se crean sistemas basados en leyes matemáticas y códigos fuentes a los que no se aplicaría los requisitos legales y fuera de control a través del que daría lugar por ejemplo a evasiones fiscales, blanqueo de capitales, desinformación o mercado negro. Con respecto a las criptomonedas el marco normativo está más maduro con el reglamento MiCA por ejemplo, porque las monedas digitales se crearon al mismo tiempo que el blockchain en la década 2010 es más antiguo mientras que los nuevos usos del Blockchain están ahora en sus fases de experimentación o incluso se están desarrollando ahora mismo

por lo cual las leyes con carácter general no están adaptadas a dichos usos y esto abre la puerta a posibles engaños.

Dentro de poco, probablemente unido a otras nuevas tecnologías, el Blockchain podría convertirse en uno de los pilares tecnológicos de la ciudad inteligente, basada en un ecosistema cada vez más integrado y automatizado y en una economía más colaborativa. Es necesario definir y clarificar las normas a escala europea y encajar esta tecnología en las legislaciones ya existentes como las normas de prevención del blanqueo, las normas sobre los procesos electorales, las normas específicas a cada sector como el sector energético en el que se hará uso del Blockchain y sobre todo, hacer buen uso de nuestros datos personales cumpliendo con el RGPD. El punto de partida de todo proyecto implementado en un Blockchain es encontrar los nuevos terceros de confianza que serán los nodos en caso de una red blockchain privada, o más bien los terceros de confianza que acreditarán la veracidad de un documento en los proyectos entorno a las identidades digitales y hacerlo encajar con las autorizaciones administrativas y con el marco normativo en general.

Todo sistema tiene sus vulnerabilidades y riesgos, pero a pesar de este, vamos a ver en este informe que el uso de DTL-Blockchain puede potenciar el bienestar a nivel local en tres niveles:

1. *La participación política:*

   A través de su aplicación en las elecciones de los representantes facilita los votos para que la gente no tenga que desplazarse a un lugar habilitado para el voto. Por otra, aumenta el interés en la toma de decisiones y en el reparto de los presupuestos participativos.

   Así, la creación de una aplicación de voto permite expresarse sobre temas que conciernen su vida cotidiana de una manera diferente y sin tener que desplazarse. Implementarla en una tecnología Blockchain es fundamental porque sustituye a los tradicionales terceros de confianza o testigo electoral que certifican que el recuento de votos se ha realizado correctamente.

   <u>Se analizará el siguiente proyecto:</u>

   - La ciudad de Neuilly en Francia experimenta el voto en línea con una DAPP basada en un blockchain. No reemplaza las boletas de papel, sino que "Neuilly

Vote" es una herramienta complementaria de diálogo con los residentes. La plataforma permite a todos expresarse sobre temas que afectan a la vida en la ciudad. (Brancato, 2021)

2. *La participación de la Sociedad Civil:*

A través de su aplicación por parte de las organizaciones no gubernamentales, fundaciones, universidades y, en general, actividades privadas sin ánimo de lucro, dichas entidades involucran los ciudadanos causas que crean que merezcan la pena como los siguientes proyectos:

- Convertir los desechos plásticos en una moneda valiosa (proyecto de Plastic Bank con IBM Blockchain Platform) (IBM, s.f.)
- Rastrear del café desde el momento en que se recolectan los granos (proyecto de IBM Food Trust) (IBM, s.f.)
- Asegurar la validez de las donaciones y la transparencia de ellas mismas. Esto tranquiliza al donante de las micro donaciones para realizar una trazabilidad cierta de su dinero y comprobar con absoluta seguridad el destino final del mismo (proyecto de la empresa española myDonor) (MyDonor, s.f.)

Se analizarán los siguientes proyectos:

- La gestión de la identidad digital: AgdataHub en Francia genera identidades digitales para el sector agrícola (particulares, empresas) que requieren la interconexión con el sistema gubernamental de identidad civil que se llama "FranceConnect". La autentificación digital de los agricultores es una cuestión crucial para el control de sus datos. Agdatahub creó una plataforma basada en un Blockchain de consorcio que garantiza que se tenga en cuenta el consentimiento de los agricultores para el uso de sus datos. Hace que el registro y la aportación de pruebas administrativas sean instantáneos y simplifica las transacciones desmaterializadas con total confianza (declaraciones electrónicas de la PAC, firma de contratos de venta de productos, etc.). (Agdatahub, s.f.)

- BCDiploma: la startup francesa digitaliza los diplomas y los aloja en un blockchain (el blockchain "Avalanche"). Esto permite que se anclen en los bloques de forma indefinida y evita posibles manipulaciones. La Universidad introduce los datos de sus alumnos o ex alumnos y únicamente ellos tienen acceso a su URL vinculado a su diploma. Pueden añadirlo a sus redes sociales (por ejemplo, LinkedIn) o enviarlo a los reclutadores. Estos últimos tienen así acceso a la prueba de la existencia de un título certificado por la Universidad. (BCDiploma, s.f.)

3. *La participación económica:*

A través de su aplicación por parte de los gobiernos, ayuntamiento o empresas, el uso del blockchain puede mejorar los siguientes sectores:

- la movilidad urbana (coches, patinetes, semáforos inteligentes, cálculos del tráfico, transporte conectado, aparcamiento, etc) como lo propone la Startup francesa Mobichain[1] y la Startup Israeli La Zooz.[2]

- El seguimiento en tiempo real del consumo de energía: el blockchain también podría utilizarse para archivar las transacciones de energía, trazadas en tiempo real, lo que permitiría una gestión más detallada y un seguimiento en tiempo real de la energía consumida (contadores, sensores), así como el intercambio de estos datos entre los distintos actores del sistema energético. Podría permitir a una comunidad tener una visión general de toda su infraestructura energética e identificar los edificios que más energía consumen.

- La gestión de activos industriales: el blockchain también puede implementarse para informar de quién es el propietario de la energía en un momento dado,

[1] Mobichain está diseñando un nuevo modelo de plataforma MaaS (Mobility as a Service), MaaS 4.0, que pone el procesamiento de datos asistido por blockchain e Inteligencia Artificial

[2] La ZooZ es una start-up israelí que ofrece un servicio de coche compartido totalmente replanteado porque está descentralizado y es propiedad de su comunidad. Este servicio de código abierto permite a conductores y pasajeros conectarse en tiempo real para llenar las plazas vacías de los conductores, sin tener que depender de un actor intermediario para la conexión: todo pasa por una plataforma autogestionada.

cuánto ha producido, vendido o comprado y cómo está evolucionando su activo/cartera de energía. Crea transparencia: propiedad y estado de las instalaciones, registro de regímenes de propiedad, etc., entre todos los actores: productores, distribuidores, autoridades locales, etc.

- Controlar los certificados en el sector energético: el blockchain se está promoviendo como respuesta a los problemas de transparencia y fraude en todo lo que gira en torno a certificados y registros: garantías de origen, certificados de metanización, créditos de carbón, etc (Think Smart Grids, 2019)

- La empresa belga Elia, junto con SettleMint y Actility, quiere construir un sistema energético que garantice la flexibilidad, fiabilidad y escalabilidad futuras. Todavía se trata de un proyecto piloto y la idea principal es implementar y automatizar los contratos inteligentes en las redes P2P. De este modo, puede ofrecer una solución escalable para reducir las barreras de entrada de los pequeños actores, por ejemplo, reduciendo la cantidad que hay que depositar para participar. (elia, s.f.)

- Eureka Confluence (barrio de la ciudad de Lyon en Francia) está experimentando un sistema de producción de energía renovable compartido por varios bloques y edificios. Los paneles fotovoltaicos y una planta de cogeneración proporcionan la producción para abastecer a los edificios de electricidad, calefacción y refrigeración. Todo el sistema se completa con un sistema de medición e información para los habitantes basado en blockchain y disponible en los teléfonos móviles. El objetivo es consumir energía renovable producida localmente. (Lyon Confluence, s.f.)

En Francia, el decreto de 28 de abril de 2017 sobre autoconsumo colectivo que modificó el código de energía, impulsó varias experiencias de autoconsumo colectivo basadas en blockchain.

Se analizará el siguiente proyecto:

- En Francia, el proyecto DIGISOL liderado por Sunchain, una spin-off de la empresa Tecsol, está experimentando con el uso del Blockchain como parte de un proyecto de autoconsumo eléctrico colectivo en la región de los Pirineos Orientales, en Perpiñán. Se basa en la Hyperledger Blockchain, una plataforma de desarrollo de Blockchain privada apoyada por la Fundación Linux. (Digisol, s.f.)

Metodología

El objetivo de mi Trabajo de Fin de Máster es investigar los buenos casos de uso de la tecnología Blockchain en las ciudades inteligentes. La finalidad es demostrar que esta tecnología innovadora puede mejorar el bienestar local de diferentes formas: mejorar la participación política local, mejorar la actividad de la sociedad civil y mejorar la actividad económica. Muy a menudo el blockchain está asociado a las criptomonedas y se desconfía de él. Por el contrario, blockchain no es una aplicación o un software, sino una estructura. Permite almacenar e intercambiar valor en Internet sin un intermediario centralizado. Por lo tanto, la cadena de bloques permite varios usos. El carácter descentralizado de las cadenas de bloques, unido a su seguridad y transparencia, promete aplicaciones mucho más amplias que las meras transacciones monetarias y, según el uso que se haga de ellas, puede mejorar nuestras condiciones de vida, permitir que las ciudades sean más eficientes energéticamente, implicar a los ciudadanos en la toma de decisiones o establecer un sistema de identidad digital seguro.

Investigué en Francia y Bélgica los diferentes casos de uso del blockchain en los 3 campos mencionados anteriormente y me puse en contacto con los diferentes responsables de estos proyectos. Un número muy reducido de ellos accedió a responder a mis preguntas, por lo cual estos casos serán los proyectos que presentaré en la sección II de mi informe. He notado que hay un gran misterio detrás del uso del blockchain ya que las empresas o los ayuntamientos contactadas no han sido muy abiertos y transparentes para hablar de su proyecto y esto por varias razones que presentaré en la conclusión. El objetivo era entender los factores que hicieron que el uso del Blockchain fuera un éxito, como la gestión de la privacidad, el mecanismo de ciberseguridad, el tipo de DLT usado, el cumplimiento de las leyes vigentes tal como al RGPD o la creación de un ecosistema de

confianza entre los ciudadanos y el uso de un Blockchain. Como punto de partida elaboré un cuestionario que sirvió para recabar la información correspondiente a cada caso que encontré y me permitió sacar los puntos clave del éxito de su implementación y sus debilidades.

Con carácter general, aunque he tenido que adaptar las preguntas dependiendo del caso, las preguntas fueron las siguientes:

Cuestiones legales	**Cuestiones técnicas**
¿Como cumplir con el RGPD? Sobre todo, el derecho de supresión, la conservación y la limitación de los datos. (La principal característica del blockchain es que los datos ingresados no son borrables ni rectificables) Por definición, el blockchain es un protocolo descentralizado, por lo cual se hace difícil designar a un responsable de tratamiento (¿será el propietario de la app usada con la tecnología blockchain, será el ayuntamiento?)	¿Qué tipo de blockchain (pública/privada/consorcio) utiliza y por qué ha hecho esta elección? ¿Como gestionar la ciberseguridad, quien accede a el blockchain y cómo / Los programadores que tienen la mano sobre este sistema? Voto electrónico: Como garantizar el anonimato y la no manipulación del voto ¿Cómo gestionar la eficiencia energética? Dado que la tecnología blockchain tiene un consumo significado ¿Se ha implementado una medida para afrontar los riesgos de exclusión de los "incompetentes" digitales ampliando aún más la brecha digital?

I. El blockchain aplicado a la mejora social a nivel local.

1. El blockchain como tecnología transformadora

1.1.Blockchain, una tecnología novedosa

Según la CNIL (Commission Nationale de l'Informatique et des Libertés) autoridad de control en materia de protección de datos en Francia:

> El blockchain es una tecnología de almacenamiento y transmisión de información transparente, segura y que funciona sin un organismo de control central. Es una base de datos que contiene el historial de todos los intercambios entre sus usuarios desde su creación, segura y distribuida: es compartida por sus distintos usuarios, sin intermediarios, lo que permite a todos comprobar la validez de la cadena. Existen blockchains públicas, abiertas a todo el mundo, y blockchains privadas, cuyo acceso y uso están limitados a un determinado número de actores. Una red blockchain pública puede compararse, por tanto, con un libro de contabilidad público, anónimo e infalsificable. Como escribe el matemático Jean-Paul Delahaye, hay que imaginar "un cuaderno muy grande, que todo el mundo puede leer libremente y de forma gratuita, en el que todo el mundo puede escribir, pero que es imposible de borrar e indestructible. (CNIL, s.f.)

El Parlamento Europeo ha llegado a definir el blockchain como: "un conjunto de bloques integrados en un sistema que comparte una base de datos común" en su Resolución nº 2016/2007 de 26 de mayo de 2016 sobre las monedas virtuales.

Esta tecnología propone una nueva estructura para alojar datos y gestionar aplicaciones reduciendo por lo tanto la necesidad de pasar por un intermediario. Las bases de datos suelen estar en mano de las empresas de la sociedad de la información poderosas, como las que manejan el Cloud (Amazon, Microsoft, Google). Así, el blockchain cambia el panorama actual porque fomenta la creación de nuevas aplicaciones menos dependiente de un órgano central. Las cadenas de bloques nos permiten almacenar datos no repudiables de forma transparente y hacerlo bajo seudónimo. Estas mismas características representan también las limitaciones más importantes de esta tecnología. Su carácter des intermediado y transnacional hace que el blockchain sea difícil de gobernar y complica cualquier cambio de su código fuente. Así vemos en su funcionamiento un peligro

inherente porque descentralizado y funcionando con diferentes mecanismos de consenso para agregar un nuevo bloque a la cadena. Luego, por ser una tecnología transparente y rastreable, podrían ser usadas por gobiernos o empresas para vigilar y controlar todo lo que ocurre en el blockchain (votos, comercio, creaciones de pasaporte, origen y trazabilidad de un producto etc). (De Filippi & Wright, 2019, pág. 44)

Los ataques del 51% se refieren a las criptomonedas que utilizan el principio Proof Of Work para validar las transacciones. Este es el caso de Bitcoin, por ejemplo. Los mineros con más potencia de cálculo tienen una mayor probabilidad de encontrar la solución que les permita validar el bloque de transacciones y obtener la recompensa. Una persona capaz de realizar un ataque del 51% tiene suficiente poder de extracción para excluir o cambiar el orden de las transacciones. Con tanta potencia de cálculo, es posible que esa persona (o grupo de personas) anule las transacciones que ha realizado y siga teniendo el control. (Bit2Me Academy, s.f.)

¿Como añadir un nuevo bloque a el blockchain?

Cada blockchain lleva su propio funcionamiento y mecanismo de consenso para añadir una información a un bloque. Es este mecanismo que permite a una red P2P añadir la información o transacción a través de personas, empresas o organizaciones que no se conocen y no confían el uno en el otro acudir a un mecanismo de consenso que será el método usado para validar un nuevo bloque. (De Filippi & Wright, 2019, pág. 52)

Entonces, el término "consenso" significa que todos los nodos de la red deben estar de acuerdo con una versión idéntica de la cadena de bloques. El mecanismo de consenso de un blockchain es en cierto modo, una auditoría interna y automática de su red que permite que se actualice y que cada bloque de la cadena es válido. Las personas que participan en la validación de los bloques (llamados "nodos" de la red) deben tener un incentivo para participar en la seguridad de la red, normalmente en forma de recompensa monetaria y por lo tanto impide que una sola entidad controle toda la red y garantiza así su descentralización. (Javier Gómez de Vera, 2022, pág. 19)

El algoritmo de consenso de Bitcoin, el Proof of Work, utiliza una cantidad significativa de recursos eléctricos para funcionar, lo que ha suscitado preocupaciones

medioambientales. De hecho, para hacer frente a este problema han surgido muchos otros mecanismos de consenso, que consumen mucha menos energía, como el Proof of Stake (PoS), el Proof of Stake Delegado (DPoS) o el Proof of Authority (PoA) (Dimitri Nitchoun y Bilal El Alamy, 2019)

PROOF OF WORK (POW) es el más utilizado de todos los protocolos de consenso de blockchain. Desde 2009, ha podido demostrar su resistencia y seguridad ante diversos intentos de ataque.

En el protocolo Proof-of-Work, los diferentes nodos de la red se denominan mineros. Para confirmar una transacción, los mineros tienen que resolver un complejo problema matemático que requiere mucha potencia de cálculo.

Para ello, utilizan un proceso matemático llamado función hash. La función hash se utiliza para escribir los datos de la transacción en bloques y conectarlos entre sí. Hay diferentes tipos de hash, como el SHA 256, que se utiliza en Bitcoin. Una vez que el hash se escribe en la cadena de bloques, es infalsificable.

Un minero es retribuido por cada bloque que consigue aprobar y confirmar. Sus ingresos son proporcionales a la potencia de cálculo que es capaz de desplegar para responder al problema. (Binance Academy, 2018)

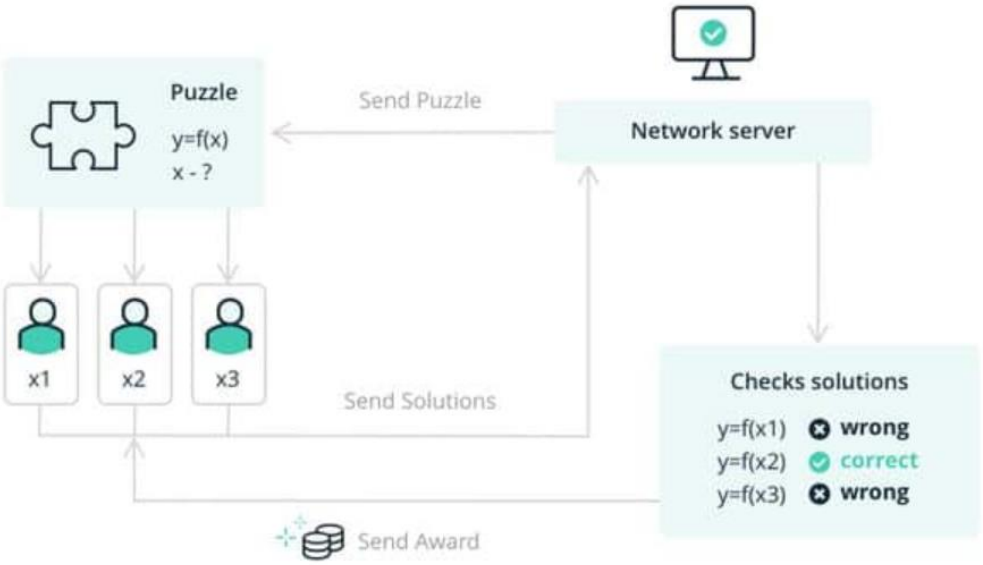

Ilustración 1: Dibujo simplificado del mecanismo de Proof-of-work

Esquema hecho por cointribune https://www.cointribune.com/es/

PROOF OF AUTHORITY (PoA) es un algoritmo de consenso basado en la reputación que crea una solución práctica y eficiente para las redes de blockchain, especialmente cuando se trata de redes privadas.

El instrumento principal en PoA no es otro que la identidad de un usuario, por lo que la validación de un bloque no implica monedas, sino la propia reputación del nodo. En otras palabras, los blockchains PoA están protegidas gracias a los nodos de validación elegidos al azar para actuar como entidades de confianza. Utiliza un número limitado de validadores de bloques, lo que hace que el sistema sea altamente escalable. Los bloques y las transacciones son verificados por participantes previamente aprobados que actúan como moderadores del sistema. Los validadores deben confirmar su verdadera identidad y un candidato debe estar dispuesto a invertir dinero y poner en juego su reputación. Un proceso difícil reduce el riesgo de seleccionar validadores dudosos y fomenta un compromiso a largo plazo con la cadena de bloques. (Bit2Me Academy, s.f.)

Ventajas	Inconvenientes
Flujo alto y rápido Más adecuado para las blockchain privadas Rapidez del consenso Alto de nivel de control de acceso porque solo los nodos con permiso pueden participar	La centralización; El PoA no está descentralizado, sino que es simplemente un esfuerzo por hacer más eficientes los sistemas centralizados Las identidades de los validadores deben ser públicas: es peligroso porque dichas personas o empresas podrían ser manipuladas por terceros Vulnerable: un usuario malicioso podría ser agregado a la lisa de firmantes

	Desbordamiento: para crear una lista de nodos validadores autorizados los nodos ya elegidos son los que tienen que votar

PROOF OF STAKE (POS) se basa en una lógica completamente diferente a la del Proof-of-Work y no requiere ninguna potencia de cálculo en particular es un consenso mucho menos costoso. En el Proof-of-Stake, los participantes en el consenso pueden ser comparados con los accionistas de una entidad comercial con el privilegio de participar en su mecanismo de consenso. En concreto, para validar un bloque, los nodos deben demostrar que poseen una determinada cantidad de criptodivisa y comprometerla con la red. Cuanto mayor sea esta cantidad, más probable será que un nodo sea elegido para actualizar el registro de la cadena de bloques. El consenso del PoS es que estas personas son las más propensas a querer luchar contra un ataque a la red, que podría arruinarlas por completo. (Bit2Me Academy, s.f.)

DELEGATED PROOF OF STAKE (DPoS) es un mecanismo de consenso que reduce el número de nodos de una red blockchain a un número reducido de validadores. Estos validadores (delegados) son elegidos por los titulares de los tokens, en proporción a lo que poseen. Los delegados definen una rotación de validadores de bloques para que todos puedan participar y ser compensados por su participación en la seguridad de la red. Esta herramienta "democrática" promueve el interés de los delegados por respetar sus compromisos y ser honestos con sus electores, que están comprometidos con la seguridad de la cadena de bloques. Por lo tanto, es posible destituir a un delegado si no respeta sus compromisos, a través de una votación. (Bit2Me Academy, s.f.)

PoS	PoA	PoW
Alto uso de energía	Bajo uso de energía	Bajo uso de energía
Riesgo de centralización	Riesgo de centralización	Riesgo de centralización

Seguridad media	Seguridad media	Seguridad alta
Transacciones lentas con altos costes	Transacciones rápidas con menores costes	Transacciones rápidas con menores costes

Conclusión:

Cada sistema tiene sus pros y sus contras, en los casos estudiados los Ayuntamientos y entidades públicas suelen elegir un blockchain público "permissioned" o de consorcio para tener un mínimo de control sobre los nodos que validan las transacciones o quien puede escribir en el blockchain. Todo reside en la elección del mecanismo de consenso. BCdiploma ha elegido un blockchain publica que funciona con PoS y esto si que es novedoso porque democrático. Todos los blockchains que no usan el PoW son mucho más ecológicos, pero disminuye el carácter novedoso del uso del blockchain a nivel local porque siguen teniendo características de un sistema centralizado, salvo el PoS que aparece como un buen compromiso democrático y descentralizado porque su funcionamiento se parece a un PoW más ecológico. En el PoA solo algunas personas o empresas pueden ser elegidas y al final, podría llegar en las manos de los mismos, es decir, los que tienen un poder económico. Pero resulta adecuado el PoA en cuanto al EBSI que nace de la cooperación entre los Estados y dedicada a los servicios públicos. En cuanto al PoS, la selección de dichas personas está vinculada también a su poder económico porque depende de cuantas criptomonedas posee. No hay una solución perfecta, no todo puede ser al 100% democrático y abierto a todos y al mismo tiempo ecológico y seguro, solemos pensar que el PoW es el más transparente y fiable, pero el PoS tiene un funcionamiento parecido con la ventaja que es utiliza menos potencia de cálculo.

- Con la PoW, la probabilidad de ser elegido para recibir el incentivo en cada periodo es proporcional a la capacidad del validador para realizar un determinado tipo de cálculo en un concurso computacional que se celebra cada 10 minutos, por ejemplo para Bitcoin.
- Con el PoS, la probabilidad de ser elegido para recibir el incentivo es proporcional a la cantidad de dinero que un validador se compromete al ponerlo en custodia, como una apuesta colocada en el centro de la mesa en una partida de póker. Esta

cantidad prometida puede perderse si pone mal la información en el bloque, hace el trabajo esperado de proponer una nueva página cuando la elección le corresponde, o si intenta utilizar sus apuestas en varios blockchains paralelos.
El dinero comprometido por un validador se recupera cuando éste desea dejar de participar. Por lo tanto, el dinero depositado es arriesgado, pero no se pierde; se devuelve a los validadores si todo va bien.

En ambos casos, un validador compromete recursos, ya sea capacidad de cálculo (POW) o fondos en custodia (POS). Si quiere estafar y multiplica sus identidades en el blockchain no le sirve de nada porque la probabilidad de ser elegido es proporcional a los recursos que arriesgados.

Al final, tras analizar los diferentes casos de usos, resultan más elegidos, democráticos, ecológicos y seguros los mecanismos de PoA y/o de DPoS. El PoW suele ser eliminado porque contradice los valores que deben transmitir las entidades públicas, padecemos una crisis ambiental grave y el minado por su potencia de calculó tiene un impacto ecológico negativo. El DPoS como el elegido por BCDiploma y la Universidad de Lille aparece como un buen compromiso porque alcanza buenos niveles de seguridad a través del algoritmo elegido para determinar los productores de bloques y verificar que los nodos son de alta calidad e individuos únicos. Al utilizar el proceso de aprobación de la votación, la red garantiza que incluso alguien con el 50% de la cantidad actual de votos no pueda elegir a un solo productor por sí mismo.

1.2.Blockchain VS DLT

Técnicamente, la principal diferencia no es entre blockchain y DLT (distributed ledger technology), sino entre DLT pública y privada.
Existen varios sistemas DLT reconocidos, como Hyperledger (IBM) o Corda (R3). Las DLT se diseñaron inicialmente para realizar transacciones en un entorno de confianza, mientras que los blockchains, herederos del Bitcoin, pretenden permitir a una comunidad de actores que no confían entre sí alcanzar un consenso sobre la integridad e inmutabilidad de un registro de transacciones común sin depender de un tercero de confianza; de ahí la expresión "sistema sin confianza". Es esta inmutabilidad la que hoy

en día es a la vez el punto fuerte y la principal debilidad de la arquitectura blockchain, que la convierte en una herramienta preferida para las transacciones financieras, al tiempo que a veces plantea problemas para la correcta ejecución del derecho al olvido y el rechazo de la intervención humana en caso de mal funcionamiento del código. (BBVA, 2018)

1.3.Tipos de Blockchain

La diferencia entre los Blockchain se hace según estén abiertas a la escritura (envío y validación de transacciones) y a la lectura (libre acceso al registro de transacciones) sin restricción de acceso al público, es el caso de una red blockchain pública que tiene carácter "abierto" o que la escritura o la lectura estén sujetas a la aceptación previa de un tercero: es el caso de una red blockchain privada, que es "cerrada".

Las denominadas redes blockchains "públicas" son accesibles a todo el mundo, siempre que los participantes cumplan el protocolo y sigan las reglas definidas por el blockchain, todo el mundo es libre de leer los datos del registro. Estos sistemas son extremadamente resistentes, ya que la base de datos es almacenada por un gran número de ordenadores.

Las denominadas redes blockchains "privadas", en cambio, están menos descentralizadas, ya que se despliegan en un marco restringido en el que sólo ciertos actores tienen derecho a leer el registro. Sólo los participantes identificados y autorizados a unirse a la red pueden acceder a la información que contiene. Se utilizarán en situaciones en las que el anonimato no es posible ni deseado.
Asimismo, es adecuada cuando no es necesario el uso de una criptomoneda o token. Los participantes están plenamente identificados. Las acciones de acceso y escritura serán sujetas a autorización, salvo la lectura que puede potencialmente ser accesible y gratis. La fuente de los datos está autentificada. También permiten gestionar de manera más precisa, la naturaleza de los datos (públicos, compartidos o privados), para encriptarlos y así garantizar una menor transferencia de datos personales y una mayor confidencialidad de los intercambios entre la red y los actores de la red.

Mientras que los blockchains privados están lógicamente "autorizados", los blockchains públicos pueden estar "permissioned" o "permissionless" en función de la posibilidad que

se ofrece a los participantes de realizar y/o validar una transacción en el blockchain. En el caso de una red blockchain pública "permissionless", cualquier puede leer los datos, firmar transacciones y modificar el registro. En el caso de una red blockchain pública "permissioned", sólo los participantes autorizados pueden escribir en él y validar los datos dentro de la cadena, aunque todos los participantes tengan derecho a leerlos. (Javier Gómez de Vera, 2022, pág. 18)

Por lo tanto, basta con tener internet para poder descargar el logicial open source que maneja un blockchain público "permissionless" para participar a la red sin desvelar su identidad. Por ser abiertas, descentralizadas y bajo seudónimo las redes blockchain "permissionless" pueden a veces ser un peligro si se utiliza en sectores regulados como la banca donde las instituciones financieras aseguran la trazabilidad de las operaciones y por lo tanto controlan a los intervinientes. Las blockchains "permissioned" ellas sufren de una falta de confianza en sus nodos ya que los miembros podrían ponerse de acuerdo para atacar al sistema. El hecho de que solamente unas personas validan y crean un bloque pueden ser más fácilmente víctimas de corrupción por lo cual es esencial seguir avanzando con los dos tipos de blockchain aprovechando de cada una de sus ventajes.

Así, blockchain públicas, privadas, de tipo "permissioned" o "permissionless" pueden mezclarse para llegar al funcionamiento deseado:

> Algunas blockchain pueden ser consideradas públicas-permisionadas, combinando los permisos asociados a consorcios privados, con un modelo de gobierno descentralizado, intentando alcanzar las mejores características de ambos modelos.
>
> También es posible la implantación de una red blockchain privada-no permisionada, es decir, una versión de una plataforma en la que cualquiera pudiera operar (leer o escribir), pero que no todo el mundo tuviera acceso a ella. (Javier Gómez de Vera, 2022, pág. 18)

Tipo de Blockchain	Nombre	Lectura	Escritura / Realización de una transacción	Validación	Ejemplo
Abierta	Publica "permissionless"	Abierta para todos	Cualquier persona	cualquiera, siempre que haga una inversión importante en potencia informática (PoW)o en la tenencia de criptodivisas (PoS)	Bitcoin (PoW) Ethereum (PoS) **Avalanche (DPoS)** **Tezos (PoS)**
	Publica "permissioned"	Abierta para todos	Participantes autorizados	todos o algunos de los participantes autorizados	Sovrin
Cerrada	Consorcio[3]	Restringida a los participantes autorizados	Participantes autorizados	todos o algunos de los participantes autorizados	Banca **Alastria (PoA)**
	Privada y "permissioned"	Totalmente privada o limitada a los nodos autorizados	Limitada al operador de la red	Limitada al operador de la red	**Hyperledger Fabric**

[3] El consorcio es una cadena de bloques que reúne a varios actores, pero no es pública ni está abierta a todos. Es una cadena de bloques híbrida por lo cual los derechos de escritura y modificación pueden modificarse y algunos nodos pueden hacerse públicos mientras otros permanecen privados

Como lo hemos visto más arriba y se deduce por lo tanto de sus características, el aspecto realmente novedoso de la tecnología blockchain reside en sus redes públicas y "permissionless". (De Filippi & Wright, 2019, pág. 40) Al final, son estas redes que aportan un real cambio en materia de transparencia y sobre todo la descentralización. Así, una empresa o un ayuntamiento que usa una red privada blockchain conserva la centralización de dichas entidades, pero mejora la trazabilidad y la inalterabilidad de las transacciones que ocurren entre los participantes. Los casos de uso estudiados en la mayoría son por lo tanto sobre blockchains públicos.

1.4.Blockchain y derecho francés

Empieza con la Orden de 8 de diciembre de 2017 sobre el uso de un dispositivo de registro electrónico compartido para la representación y transmisión de valores financieros.

El termino Blockchain fue introducido en la legislación francesa por el Decreto nº 2018-1226, de 24 de diciembre de 2018, sobre la utilización de un dispositivo de registro electrónico compartido para la representación y transmisión de valores financieros y para la emisión y transferencia de "miniobligaciones". De cara al futuro, entre 2016 y 2019, Francia se ha comprometido a poner en marcha un marco jurídico completo para las tecnologías blockchain y sobre todo, los activos digitales.

Como primera medida, se autorizó el uso de un dispositivo de registro electrónico compartido mediante una orden de 28 de abril de 2016 para la transferencia de "minibons".

Los "minibons" son productos de inversión emitidos por las SAS, SA o SARL cuyo capital está totalmente desembolsado. El inversor (particular o empresa) hace un préstamo a la empresa y recibe a cambio un bono (reconocimiento de deuda), amortizable en una fecha determinada.

Así, para adaptarse al blockchain, se ha modificado el código "monétaire et financier" (Código de Comercio francés), modificando los artículos siguientes:

Article R211-1	"Los valores financieros se acreditarán únicamente mediante una anotación en la cuenta de valores de su(s) propietario(s) o en beneficio de éste(s) en un dispositivo de registro electrónico compartido."
Article R211-3	"Cuando el mantenimiento de las cuentas de valores o el registro de valores en un dispositivo de registro electrónico compartido sea responsabilidad del emisor y éste designe a un agente para este fin, publicará en el *Bulletin des annonces légales obligatoires* el **nombre y la dirección** de su agente, así como la **categoría de valores financieros** que es objeto del mandato."
Article R211-4	"Un propietario de valores financieros registrados puede **encargar a un intermediario** contemplado en el artículo L. 211-3 el mantenimiento de su cuenta de valores en un emisor o la gestión de las anotaciones en el dispositivo de registro electrónico compartido contemplado en el mismo artículo. En este caso, las anotaciones en esta cuenta de valores o en el dispositivo de registro electrónico compartido **figurarán también en una cuenta de administración** mantenida por este intermediario. El titular de la cuenta de valores se compromete a dar órdenes sólo a este último."
Article R211-5	"Las participaciones o acciones de los organismos de inversión colectiva y los instrumentos de deuda negociables pueden negociarse en un centro de negociación de forma registrada **sin haber sido necesariamente colocados en una cuenta de administración, siempre que estén registrados en un dispositivo de registro electrónico compartido**."
Article R211-9-7	"El sistema de registro electrónico compartido a que se refiere el artículo L. 211-3 deberá diseñarse y aplicarse de forma que garantice el registro y la **integridad de las inscripciones** y permita, directa o indirectamente, **identificar a los propietarios de los valores y la naturaleza y el número de valores que posean.** Las inscripciones realizadas en este servicio de registro estarán sujetas a un plan de continuidad de la actividad actualizado, que **incluirá un servicio de conservación de datos externo."**
Article L54-10-1	"2° Toda **representación digital de valor que no sea emitida ni garantizada por un banco central o una autoridad pública**, que no esté

Define los activos digitales	necesariamente vinculada a una moneda de curso legal y que no tenga el estatuto jurídico del dinero, pero **que sea aceptada por personas físicas o jurídicas como medio de intercambio** y que pueda ser transferida, almacenada o intercambiada electrónicamente"
Article L552-2 Sobre los Tokens	"Un token es cualquier activo intangible que representa, en forma digital, uno o más derechos que pueden ser emitidos, registrados, almacenados o transferidos por medio de un dispositivo de registro electrónico compartido que permite identificar al propietario del activo, directa o indirectamente."
Article L211-3	"El registro en un dispositivo de registro electrónico compartido **se considerará una inscripción en cuenta**."

Fuente: Código "monétaire et financier"

Los últimos artículos del código financiero proporcionados en la tabla más arriba muestran que dentro de la categoría de activos digitales a los que se aplica la regulación de los proveedores de servicios de activos digitales encontramos, por un lado, los tokens, excepto los que reúnen las condiciones de los instrumentos financieros, y por otro lado, las criptomonedas.

La ley francesa define la criptomoneda como una representación digital de un valor, perteneciendo a un género propio al no tener la condición jurídica de dinero por sus características particulares. Luego, los tokens son activos digitales que constituyen una herramienta de financiación para las empresas, en particular en el contexto de la recaudación de fondos de criptomonedas conocida como "ICO" (oferta inicial de monedas).

En la práctica, las empresas emiten tokens que posteriormente se intercambian con los inversores por criptomonedas. Estos tokens pueden dar derecho a diferentes beneficios como títulos, derechos de voto, beneficios, dividendos o incluso acciones.

Para concluir, a partir de la citada Orden, se ha creado la inscripción en un registro distribuido, que coexiste con el sistema tradicional de registro de cuentas. Por lo tanto, el legislador ha asimilado jurídicamente estas dos operaciones, como se estipula en el artículo L211-3 (la inscripción en un blockchain sustituye a la inscripción en cuenta

tradicional). En consecuencia, el uso de un blockchain o DLT constituye una modernización de los métodos de mantenimiento de las "cuentas de valores" de los accionistas, especialmente para las empresas con un gran número de accionistas y/o las que gestionan grandes movimientos de valores o fondos (gestores de activos, plataformas de crowdfunding, etc.)

Entonces, el blockchain tiene una definición legal pero muy limitada porque hasta ahora, está muy ligada al sector financiero y a las criptomonedas. Hay un vacío legal del uso de dicha tecnología en los otros sectores como el de los votos en línea, de las donaciones, de la movilidad urbana etc, aunque en el sector energético no se menciona el blockchain en sí pero si se deduce que se pueda usar dicha tecnología porque se debe "aplicar las medidas técnicas y contractuales necesarias, en particular en lo que respecta a la medición de la electricidad, para permitir que las operaciones de autoconsumo se realicen en condiciones transparentes y no discriminatorias"[4] que veremos a continuación en el último caso sobre DIGISOL y SUNCHAIN.

2. El blockchain aplicado al ámbito local: Usos públicos y privados

2.1. El uso del blockchain por las Administraciones: un reto técnico y legal

La construcción de la red subyacente tendrá que responder en el ámbito público a las especificidades del sector o procesos (procedimiento y regulación) pero también del ecosistema y la gobernanza propios de cada país y administración.
El uso del Blockchain por parte de las Administraciones tiene sus límites en cuanto al enfoque que tiene que respetar las entidades públicas como lo niveles de seguridad a implementar. "La Administración Pública sirve con objetividad los intereses generales" (artículo 103.1 de la Constitución española). Aunque usen una tecnología blockchain, las Administraciones deberán actuar según las prerrogativas que el ordenamiento jurídico les atribuye respetando la Constitución y las leyes como la LPAC y la LRJSP.

Las doctrinas discrepan y consideran por un lado que "La tecnología blockchain impulsará el ejercicio compartido de las potestades públicas entre aquella y los agentes privados" y por otro lado que "en el sector público tan solo podrá

[4] Artículo L.315-6 del Código de Energía francés.

plantearse en términos realistas la utilización de redes privadas o no permisionadas, que son las que, precisamente, representan un menor avance desde la perspectiva tecnológica." (Cárceles, 2019) Entonces, la tecnología blockchain en el seno de las Administraciones no puede llegar a un mejor reparto de las potestades públicas y a más transparencia si se usa un blockchain privado por las mismas razones que vimos más arriba, sigue siendo centralizado y en manos de unas pocas personas. Es mucho más relevante y novedoso por parte de una Administración usar un blockchain público, pero teniendo cuidado con el mecanismo de consenso para adecuarse al máximo con el propósito final.

Luego, según el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas deben respetar el Esquema Nacional de Seguridad.

Así, al principio parece muy difícil por una administración pública elegir una red pública, aunque si es posible proteger la identidad de las personas que realizan las transacciones a través de un sistema de criptografía asimétrica mediante una clave pública y la otra privada. Así, el titular de una transacción decide de quien puede acceder a la misma o no, cifrando el mensaje de tal forma que su contenido sea consultado solo para aquellos nodos que dispongan de la clave privada del emisor. (Ponce de León, 2018, pág. 44). En todo caso, implementar medidas de seguridad adecuadas en el sector público supone inversiones muy relevantes, por la formación del personal y por las medidas de seguridad en sí misma por lo cual es un reto técnico y necesita dinero.

En España, el articulo 9.2 c) LPAC señala que, en sus relaciones con la Administración pública, cualquier interesado pueda identificarse utilizando "cualquier otro sistema que las Administraciones Públicas consideren válido". Así, el uso de blockchain como método de identificación ante la Administración pública parece compatible con el sistema jurídico administrativo. En este sentido, el art. 42 LRJSP permite utilizar el sello electrónico o el código seguro de verificación, eso "consiste en la identificación alfanumérica de un documento, cuyo original queda custodiado por un tercero de confianza en un servidor web." (Cárceles, 2019)

El blockchain aplicado a la acción administrativa tiene sus dificultades en cuanto a la introducción de modificaciones ya que los ciudadanos tienen el derecho a "ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones" (LPAC, art 13. e). En este sentido, el RGPD supone un problema también con respecto al ejercicio de los derechos de rectificación de la información y supresión.

En su libro blanco publicado en 2021, especialistas del sector tecnológico, legal y profesores de la Universidad de Lille (Francia) intentaron mostrar que el sector público puede beneficiarse de las características únicas que ofrecen las tecnologías blockchain, respetando sus valores y ofreciendo una mejor experiencia y mayor confianza a los usuarios de servicios públicos franceses y europeos. En este documento, explican que:

> El blockchain se considera una infraestructura de red entre pares en el que se ejecutarán las aplicaciones transaccionales que pueden estar en modo:
>
> ● G2G - Government to Government (por ejemplo, entre diferentes administraciones nacionales y transnacionales u organismos públicos)
> ● G2C - Government to Citizen (entre una administración y un ciudadano)
> ● C2C - Ciudadano a Ciudadano (entre ciudadanos incluyendo un elemento de servicio público)
>
> Los organismos públicos son los principales intermediarios de estas transacciones y los garantes de su buen funcionamiento. Los documentos que emiten o certifican son el medio habitual para verificar la información sobre las personas (documentos de identidad, permisos de trabajo, permisos de conducir, etc.) y mercancías (origen de los contenedores, seguridad de los productos, etc.).
>
> En comparación con las bases de datos centralizadas tradicionales, el blockchain garantiza dos características específicas:
>
> ● La integridad y la trazabilidad en tiempo real de los datos, para la colaboración eficiente y transparente entre los usuarios, sin el uso de un tercero externo de confianza;

- Auto ejecución de contratos inteligentes para automatizar y asegurar los procesos lo que se traduce en ganancias de eficiencia y calidad. (de Coëtlogon, y otros, 2021, pág. 14)

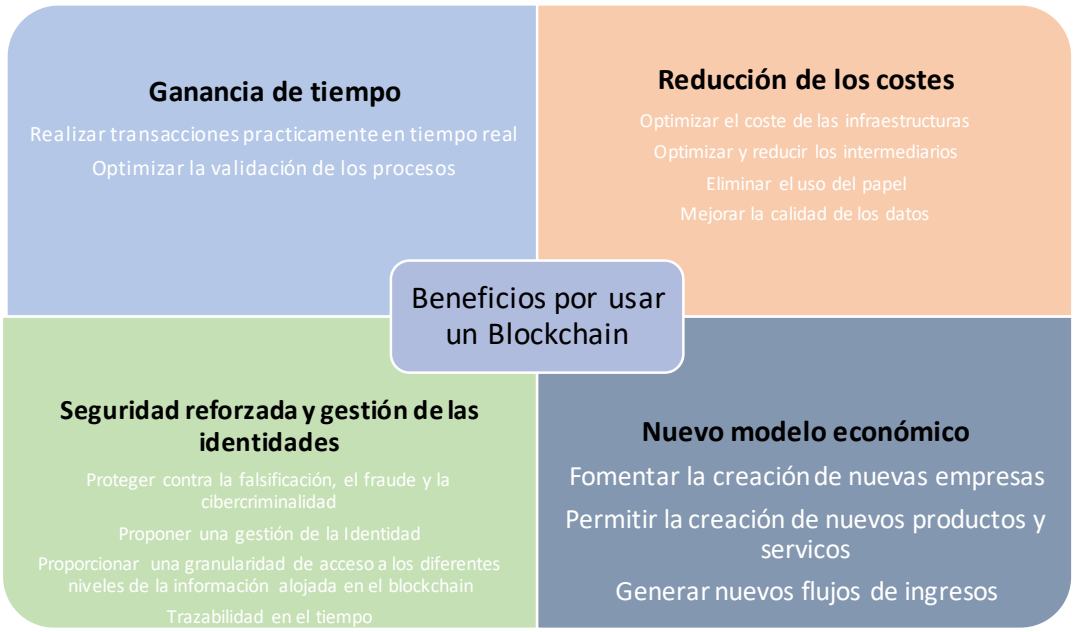

Ilustración 2: Beneficios por usar un blockchain
Fuente: Información tomada de la empresa Kapalt.
Diseño y traducción propios.

2.2 EBSI, la infraestructura europea de servicios blockchain adaptada al sector público

La infraestructura europea de servicios blockchain (EBSI, por sus siglas en inglés) es un ejemplo concreto de blockchain para el sector público. Las Administraciones pueden integrarlo en su propia estrategia de transformación digital y beneficiarse de una serie de herramientas. La idea es proporcionar confianza a través de una infraestructura europea única gestionada conjuntamente por las instituciones públicas de los diferentes países de la unión europea. El EBSI no se centra en crear tecnología, sino en crear una red utilizando tecnologías disponibles y probadas tecnologías disponibles y probadas, complementándolas si no son suficientes. (EBSI, s.f.)

NB: El blockchain EBSI sigue siendo experimentado, todavía no lo podemos usar.

Basado en dos protocolos de código abierto, la primera versión del EBSI se lanzó en julio de 2020 en una fase piloto. Hyperledger Fabric e Hyperledger Besu incorporan un

algoritmo de validación de PoA. Los nodos son instalados y probados en todos los Estados miembros por organizaciones autorizadas. RENATER lleva los primeros nodos EBSI para Francia. En España, uno de los nodos de la red EBSI está en las instalaciones de la SGAD (Secretaría General de Administración Digital) y el otro está en RedIris (la red para Interconexión de los Recursos Informáticos de las universidades y centros de investigación).

La clave de este blockchain reside en el funcionamiento de sus capas. Los especialistas que escribieron el libro blanco citado más arriba destacan que el hecho de poder modelar y adaptar el blockchain en función de su finalidad la vuelve muy atractiva para el sector público.

> En el ámbito del sector público, la cadena de bloques europea EBSI desempeña un papel fundamental. Proporciona un marco flexible para las capas 1 y 2, al tiempo que garantiza el estricto respeto de la privacidad, la seguridad de los datos y las normas de cumplimiento. Cualquier usuario o parte interesada del servicio público se beneficiará en términos de confianza, transparencia y eficiencia operativa a través de las aplicaciones puestas a disposición en la capa 3, mientras que la integración con los activos de aplicaciones existentes en la capa 4 será posible. (de Coëtlogon, y otros, 2021, pág. 23)

Los aspectos técnicos se detallan en la documentación del sitio: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI

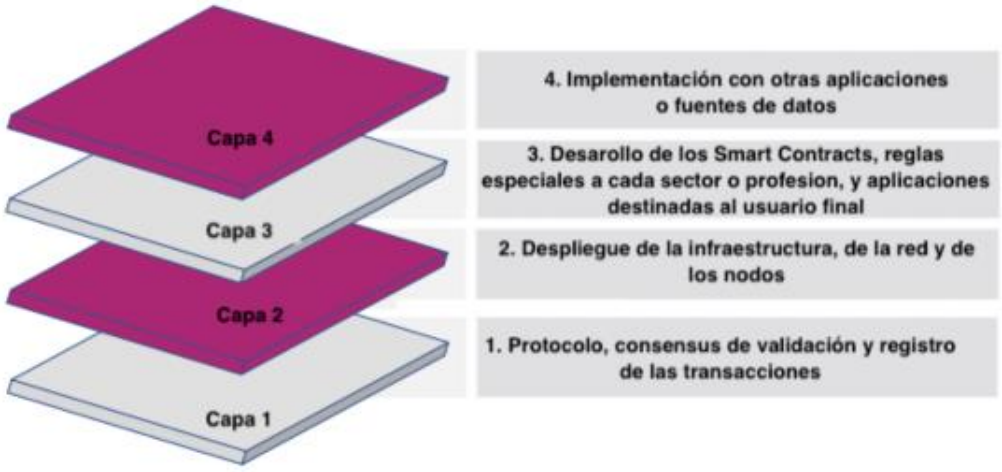

Ilustración 3: Representación global de un proyecto implementado en blockchain según sus capas tecnológicas.
Fuente: Información y diseño tomados de la empresa Kapalt.

Traducción propia.

La esencia de la versión 1 del blockchain EBSI reside en la elección de un algoritmo de validación mucho más estatal o del poder ejecutivo que es la prueba de autoridad (PoA). A diferencia de otras redes blockchain como Bitcoin (PoW) o Tezos (PoS) cuya confianza reside exclusivamente en los algoritmos de consenso/validación, parece muy adecuado usar una PoA porque permite al Estado, y por extensión a sus administraciones y delegaciones de servicio público u otros actores, el derecho a convertirse en nodos validadores de datos y a escribir eventos (transacciones) en el registro de forma inmutable e irrevocable, reflejando un cambio en el estado de los datos del servicio público. La versión 2 que está en prueba se añade un nuevo protocolo integrando una implementación del algoritmo Proof of Stake (PoS), que permitirá trabajar en la interoperabilidad de al menos dos modelos de blockchain. (de Coëtlogon, y otros, 2021, pág. 24)

Europa depende bastante de los gigantes tecnológicos estadounidenses y chinos por lo que se plantean cuestiones de soberanía digital en relación con la dependencia europea en los ámbitos público y privado. En un contexto de aceleración de la transformación digital, la elección de las tecnologías e infraestructuras sobre las que los Estados europeos construirán sus futuros servicios públicos es crucial y en particular, la infraestructura Cloud y por lo tanto la gestión de los datos de los ciudadanos europeos. Así, hay que tener en cuenta que, aunque la digitalización de los documentos facilita y simplifica la vida diaria de los ciudadanos, aumenta por lo tanto el flujo de informaciones y deja abierta la puerta para las actividades fraudulentas porque sin las herramientas digitales adecuadas, los documentos digitales siguen siendo relativamente fáciles de falsificar. (von Blücher, 2022)

En conclusión, su infraestructura modulable y sus nodos validadores, elegidos por los gobiernos, ubicados en los países miembros y por lo tanto de confianza, permiten a las Administraciones según el Libro Blanco:

> Ofrecer mejores servicios integrados a los usuarios y a las empresas, tanto en su propio país y en la Unión Europea.
>
> Mejorar la transparencia y la confianza en los servicios públicos.
>
> Simplificar los procesos administrativos y aumentar la eficacia.
>
> Aumentar la seguridad y confidencialidad de los datos.

> Garantizar la sostenibilidad, portabilidad y viabilidad de los datos. (de Coëtlogon, y otros, 2021, pág. 29)

Los proyectos desarrollados sobre el EBSI están centrados sobre todo en la creación de una identidad digital, es decir, generar un mecanismo que tendremos en nuestro smartphone como si fuera nuestra cartera "física", teniendo el DNI, el carnet de conducir, la tarjeta sanitaria, etc.

II. Análisis de casos prácticos de uso de blockchain para la mejora social a nivel local

1. Blockchain aplicado para la mejora de la participación política local:

1.1. Panorama general

El Blockchain también puede facilitar y democratizar el proceso electoral. En lugar de dar a las autoridades electorales y demás plena autoridad para contar, registrar y verificar los votos, los ciudadanos pueden votar de forma anónima y recibir copias de sus votos que no pueden ser manipuladas por los gobiernos en un sistema inmutable de blockchain. Es decir, el blockchain puede mejorar fundamentalmente las condiciones de votación. Por cierto, los procedimientos electorales basados en blockchain son una realidad en Estonia desde 2005. (Izquierdo, 2019)

Se debe tener cuidado con los datos alojados en un blockchain ya que suele haber confusión sobre qué es realmente un dato personal y, por lo tanto, la aplicación del RGPD siendo insuficiente la técnica de seudonimización para eximirse de este cumplimiento normativo.

Así, la Comisión Europea señala lo siguiente:

> Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.
>
> Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona,

siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD.

Los datos personales que hayan sido anonimizados**,** de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible. (Comisión Europea, s.f.)

1.2.Proyecto "Neuilly Vote" del Ayuntamiento de Neuilly-sur-Seine, Francia

En colaboración con Electis[5], una asociación sin ánimo de lucro, Neuilly-sur-Seine se está dotando de una infraestructura de voto digital cuyo código informático público está basado en software de acceso abierto, tecnologías criptográficas recientes y un blockchain francés Tezos.

Cuestiones preliminares:

Podemos hacer transferencias o pagar los impuestos en línea, pero para poder votar en línea el reto está en la voluntad de tener todo anónimo. Por un lado, debemos estar seguro del canal en el que mandamos nuestro voto, por el otro estar seguro de que nadie puede ver la composición de nuestro voto, que no sea vinculado a nuestra identidad.
Con el uso de una App de voto y del blockchain, la meta es permitir al votante verificar que su voto está en la "urna electrónica", con la buena información pero que nadie más lo pueda hacer y que por fin podemos contar los votos como si fuera en papel.

¿Por qué el Blockchain Tezos?

Para lograr su consenso, Tezos implementa la Proof of Stake. Esto significa que los miembros de la red bloquearán una parte de sus tokens, que ya no podrán utilizar, para obtener el derecho a crear un bloque. El creador de un bloque será elegido al azar entre todos los candidatos según el número los tokens que tiene.

[5] Electis es una asociación sin ánimo de lucro dedicada a la promoción del voto electrónico de nueva generación. No político y no comercial, Electis se apoya en una comunidad y facilita proyectos concretos de votación. Dos primeros proyectos están previstos para 2020: una votación internacional interuniversitaria y una votación de los jóvenes durante la COP26.

Más concretamente, el mecanismo implementado es el Liquid Proof of Stake (LPoS). La cantidad de XTZ que hay que poseer para convertirse en panadero o "baker" es significativa (8000 XTZ como mínimo) y no está al alcance de todos. Por lo tanto, es posible que los titulares más pequeños deleguen su XTZ a un panadero para reforzarlo (no se trata de "dar" su XTZ a un panadero, sino de "depositar" su XTZ a favor de un panadero. Puede retirar su delegación o cambiar de panadero delegado en cualquier momento). A cambio, el panadero redistribuirá entre sus delegados una parte de sus ganancias por la cocción, en proporción a su participación.

El proyecto:

El primer experimento toca el sector de la cultura y permite a los usuarios de la mediateca y del cinema de la ciudad votar en línea para elegir los libros/películas que quieren descubrir.

Luego, otros proyectos municipales estarán abiertos a consulta: por ejemplo, podrá votar para decidir las fechas de las obras o para la apertura de determinados horarios de sus instalaciones públicas. Es muy importante destacar que no se hace para los votos importantes como pueden ser las elecciones del alcalde o presidenciales por lo cual descarta el cumplimiento de las leyes sobre el régimen de las elecciones. La meta es abrir nuevos canales de votos para fomentar la participación ciudadanía donde no se vota hoy en día. Para que toda la gente pueda votar y participar en estas decisiones, en la mediateca de Neuilly han puesto Ipad en libre acceso para que los habitantes que no tuvieran internet pueden votar. Por ahora las consultas están de libre acceso a cualquiera, no solo a los habitantes de Neuilly. Funciona con una dirección de correo únicamente para meterse en la página "NeuillyVote" y registrarse para votar en línea; la última consulta fue para apoyar a un autor que participa en la selección del Premio Goncourt 2022.

En cuanto a la solución de voto electrónico de código abierto Electis.app usada en este caso, sus creadores Gilles Mentré y Franck Nouyrigat han decidido dejarlo "Open source" para que cualquier experto o ingeniero lo pueda ver y examinar por lo tanto eso genera confianza por parte de los ciudadanos, y por otra parte para aceptar toda ayuda y mejora del sistema.

Así, tener un logicial en “Open Source” genera desafíos y anima a los expertos del mundo a buscar fallos, encontrar mejoras y por lo tanto impulsar el desarrollo de dichas tecnologías novedosas.

El blockchain como tecnología adecuada para alojar la aplicación de voto en línea:

El blockchain permite emitir un informe electoral "inteligente". Sustituye a los tradicionales asesores que certifican que el recuento de votos se ha realizado correctamente. Estas actas se elaboran de forma automática, transparente y descentralizada, no hay intervención humana entre el momento del recuento de los votos y el momento de la publicación del resultado. Por lo tanto, podemos estar absolutamente seguros del resultado.

La App garantiza el anonimato de los votos y la privacidad de los votantes:

A diferencia de las encuestas y consultas públicas, el voto es anónimo. “Neuilly Vote” no vincula públicamente una papeleta a un votante, lo que garantiza el anonimato del voto. Como segundo nivel de seguridad, los votos están encriptados y no pueden ser leídos individualmente. Al utilizar el cifrado “homomórfico”, Neuilly Vote sólo puede descifrar los resultados (es decir, la suma de los votos) sin conocer nunca cada voto en particular. Por último, cuando se organicen elecciones, las claves de cifrado se entregarán a los garantes oficiales, que son los únicos que pueden abrir, cerrar y validar las elecciones. Todo ello se publicará en la cadena de bloques y, por tanto, podrá ser consultado en forma de registro digital. Según Gilles Mentré, CEO de Electis, “a través de la criptografía, el voto desde que entra en el servidor se desprende de la identidad del votante y se convierte en un voto anónimo que será contabilizado como tal".” (Brancato, 2021)

El resultado de una elección puede ser contestado:

En primer lugar, cada votante puede comprobar que se ha tenido en cuenta su voto.
Neuilly Vote también permite realizar auditorías externas que garantizan el procedimiento de votación (recuento). Por último, los garantes de la elección pueden decidir renovarla o anularla. La ventaja del voto electrónico es su rapidez y su bajo coste, en comparación con la logística necesaria para las consultas en papel.

No obstante, el voto en papel no desaparece.

Conclusiones:

Así, la criptografía y sobre todo en este caso, el cifrado homomórfico puede descifrar el resultado de los votos como conjunto, pero no cada uno individualmente. Gracias a la tecnología blockchain, se publica al mismo tiempo el conteo de votos y el resultado, es decir no hay plazo entre el conteo y la publicación de los resultados. Además, se puede ver el enlace a estos votos permitiendo rehacer el conteo, descifrando los votos a partir de las llaves de criptografía.

Cuando votamos, no confiamos en el pequeño trozo de papel en sí, sino en los presidentes de mesa y los vocales. Es una confianza descentralizada, confiamos en las personas que se encargan de los procesos electorales o porque las conocemos o porque hubiera podido tener este cargo, o que las hemos elegido etc. Ahora bien, en el caso de "Neuilly Vote", es muy importante subrayar que hay unos "e- asesor" / "e-vocales", y lo que hacen es a partir del listado de los votos (del Hash) verificar que hay en la urna la misma cantidad de votos que de personas que votaron. Luego, si poseen la llave para descifrar los votos pueden acceder a la información y por lo tanto sacar el resultado.

Gilles Mentré explica que su idea es permitir el voto en línea, pero manteniendo el formato papel (igual que en Estonia, entre 6 y 2 días antes de las elecciones pueden votar electrónicamente, y el día de la votación las personas que no hayan votado telemáticamente pueden votar presencialmente). Hoy en día, una parte de los ciudadanos creen y sienten que votar no es tan útil por lo cual el voto en línea, sin abandonar al voto papel, parece dar respuesta a la crisis democrática actual en el sentido de que involucra y escucha la voz de los ciudadanos.

(Neuilly-sur-seine, s.f.), (Vignon & Mentré, 2022)

2. Blockchain aplicado para la mejora de la sociedad civil a nivel local

2.1. Panorama general

Diseñado inicialmente para el ámbito de las monedas y los activos digitales (NAKAMOTO, 2008), el blockchain está iniciando una transformación fundamental en la forma de y las organizaciones pueden demostrar su identidad y generar confianza en

línea. En 2015, los gobiernos de Estados Unidos[6] y Estonia[7] aprovechaban el potencial de esta tecnología para la gestión de la identidad digital descentralizada.
Las crisis económicas provocadas por las guerras, las catástrofes naturales o la corrupción no permiten a las personas disfrutar de su derecho a un nivel de vida adecuado. Como consecuencia, países como el Venezuela o el Salvador, cuya moneda nacional está devaluada en un 96%, están recurriendo a las criptomonedas basadas en el Blockchain como solución. (Comben, 2020)

Además, en tiempos de guerra, la pérdida o destrucción de las tarjetas de identificación de los refugiados puede dificultar la obtención de la identidad (ser reconocidos: quiénes son y de dónde vienen) en un país de acogida y el derecho al reconocimiento como persona ante la ley (artículo 6 de la Declaración Universal de los Derechos Humanos) puede ser violado. Para resolverlo, el sistema de identidad basado en blockchain, que elimina la necesidad de documentos físicos, tiene el potencial de crear nuevas soluciones para los sistemas de identificación de refugiados. (Morrow)

Por último, desgraciadamente, los bienes civiles, como escuelas, hospitales o casas, son a veces destruidos en guerras o catástrofes naturales. Resulta muy difícil demostrar la propiedad cuando las organizaciones gubernamentales que conservan los títulos de propiedad también son destruidas. Una situación similar se produjo cuando un catastrófico terremoto devastó Haití en 2010 dejando a millones de personas sin hogar. En consecuencia, los propietarios no podían demostrar que eran los legítimos dueños de sus tierras.

Por estas razones la digitalización de los documentos físicos a través de la tecnología blockchain puede ayudar a un propietario demostrar su propiedad a través de títulos de propiedad basados dicha tecnología incluso si pierde su copia del título o se ve obligado a abandonar su propiedad. Dado que el sistema blockchain permite obtener pruebas digitales accesibles y seguras (títulos de propiedad en este caso), podría ser una solución

[6] El 16 de diciembre de 2015, la División de Ciencia y Tecnología del Departamento de Seguridad Nacional de los Estados Unidos publicó una beca de investigación para la innovación titulado: La aplicabilidad de la tecnología Blockchain a la gestión de la identidad relacionada con la privacidad
[7] International Business Time, Bitnation y el gobierno de Estonia comienzan a difundir la jurisdicción soberana en el blockchain. Febrero de 2016

para la protección de los derechos de propiedad en estas situaciones. (Accenture, s.f.) (Accenture Technology, 2018)

2.2. Proyecto Agri-consent por Agdatahub, Orange Business Services e IN Groupe

El proyecto:

- Vincular la identidad de los agricultores a la identidad de su explotación para garantizar un intercambio de datos fiable, seguro y trazable
- Garantizar con carácter general la identidad de las personas que intervienen sobre los flujos de datos en el sector agrícola creando un ámbito de confianza que permita mandar datos, certificados o pagos a la persona adecuada.
- Registrar las transacciones de este consentimiento que se aparenta en un contrato entre 3 partes: la persona que facilita el dato, la persona a quien pertenece el dato y por último, la persona que usará el dato.
- El sistema de identidad digital descentralizado utiliza un blockchain de consorcio (Alastria) y está alojado en la nube pública de Orange Business Services

Garantizar la identidad: Una vez que el agricultor se autentifica como propietario de la explotación, su certificado de identidad digital agrícola puede añadirse sencillamente a un monedero digital directamente en su teléfono. Esta prueba de identidad, a la que se puede acceder mediante un código QR, puede utilizarse entonces para los intercambios con los proveedores, los clientes, la Administración o las autoridades. Los participantes pueden utilizar instantáneamente verificar la autenticidad de la explotación y comprobar que el agricultor es su legítimo propietario.

Registrar el consentimiento sobre el uso de sus datos: El agricultor también mantiene el control sobre cómo se utilizan sus datos y a quién se le da permiso para acceder a ellos. Puede añadir o retirar permisos, lo que significa que puede intercambiar los datos elegidos con cualquier parte interesada de su elección. Esto agiliza los procesos, como las declaraciones de impuestos en línea, los contratos de venta con la industria agroalimentaria o la gran distribución, y las compras de suministros, y reduce en gran medida el riesgo de fraude. (Orange Business Services, s.f.) Todos los días, los agricultores generan una gran cantidad de datos, por las maquinas que usan, los productos

para fertilizar los suelos y otros, estos datos son hoy en día conectados. Proporciona datos de rendimiento, calidad de los productos o de clima. Estos datos pertenecen a los agricultores y para poder explotar dichos datos es necesario pedir permiso al agricultor. Cuando recibe esta solicitud de acceso, el agricultor puede aceptar o rechazar el envio del dato solicitado. Este consentimiento es el dato que está registrado en Alastria y hace posible consultar estos consentimientos a lo largo del tiempo cuando sea necesario.

Ilustración 4: El funcionamiento de Agdatahub según sus capas tecnológicas
Fuente: Esquema extraído del Libro Blanco de la Universidad de Lille, traducción propia

Las capas 1 a 3 representan la infraestructura, que no utiliza el EBSI, pero la idea es su futura interoperabilidad con el EBSI.
La capa 2 no es exclusiva de Orange Business Services y se abrirá a otros proveedores de la nube. Los proveedores podrán ofrecerse para alojar nodos y permitir una descentralización más completa de la arquitectura. (de Coëtlogon, y otros, 2021, pág. 45)

Conclusiones:

Así, esta aplicación AgriConsent y el hecho de implementarla en el blockchain de consorcio Alastria permite acreditar su identidad y sus títulos, certificados agrícolas frente a terceros. El Wallet que posee el agricultor le permite compartir con terceros socios credenciales digitales que contengan información sobre el propietario de la aplicación (apellidos, nombre), la entidad legal (nombre de la empresa, número Siret) y los derechos que vinculan a ambos (papeles).

La clave es crear un entorno de confianza lo que por consecuencia ayudará al agricultor en sus intercambios y ventas con los clientes. Luego beneficiará a la sociedad en general porque nos permite verificar de forma extremadamente segura sus certificados que sean del agricultor en sí o de la persona moral. Así podemos saber si respecta las normas sanitarias por ejemplo el certificado "Certiphyto".[8] De igual manera nos permite verificar que los productos Bio no son estafados ya que posee la certificación que previamente ha sido concedido por una autoridad competente o de confianza dependiendo del certificado como el ministerio de agricultura y la entidad "FranceConnect"[9]. Es decir, el Wallet del agricultor en Agriconsent permite la creación de una identidad digital acreditada por France Connect y la obtención de credenciales digitales emitidas por la plataforma "Registres des Actifs Agricoles", una plataforma que registra los activos agrícolas.

En cuanto a los datos personales, no están tratados en el blockchain sino en la aplicación instalada en el teléfono móvil del agricultor únicamente, que por lo tanto tiene el control de su información personal (literal y figuradamente). Sólo se registran en el blockchain las pruebas de entrega de estos atributos, no la información que los compone (nombre, apellido, nombre de la empresa, etc.). Tampoco hay problemas respecto a la designación de un responsable de tratamiento en el blockchain porque no se tratan daos personales en dicha estructura.

Sobre la estructura, Alastria es un blockchain de consorcio para poder elegir a las personas que participen en el proceso de verificación de transacciones y también para el medioambiente ya que el consensus se logra con una PoA. (Agdatahub, 2022)

De lo anterior se puede indicar que, si bien la empresa afirme que no realiza tratamiento de datos alguno en la blockchain, a la luz de la definición de la Comisión Europea sobre el concepto de datos personales los "verifiable credentials" de llegar a identificar al agricultor podrían considerarse datos personales. Probablemente, el consentimiento sobre

[8] Desde 2015, todos los profesionales que trabajan con productos fitosanitarios, independientemente de su condición o sector de actividad, están obligados a poseer el Certiphyto. Este certificado acredita conocimientos suficientes para utilizar los plaguicidas de forma segura y reducir su uso, pero no constituye una cualificación profesional.

[9] FranceConnect es un dispositivo de autenticación digital que garantiza la identidad de un usuario a los sitios o aplicaciones de los usuarios apoyándose en las cuentas existentes cuya identidad ya ha sido verificada.

el reparto de sus datos es decir, el "acepto" o "rechazo" el acceso a un dato por ejemplo de rendimiento, podría ser vinculado a su identidad y almacenado en una base datos, en tal caso, se hace un tratamiento de datos personales que conllevaría el cumplimiento del RGPD.

2.3 Proyecto Fr.EBSI: una primera experimentación del caso de uso de "Diploma" en el Servicio Europeo de Infraestructura de Blockchain (EBSI) apoyada por el Ministerio francés de Educación Nacional, Juventud y Deportes.

El proyecto:

Este proyecto muy novedoso que tiene vocación a largo plazo usar el blockchain EBSI tiene como objetivos:

- La emisión de "Verifiable Credential[10]" en formato W3C/EDCI
- La implementación de identificadores de identidad descentralizados vinculados a las credenciales
- El estudio de las implicaciones legales, reglamentarias y organizativas del uso del blockchain

Por ahora, el proyecto que ya está en su fase experimentación lo lleva 3 entidades:

- La Universidad de Lille coordinó el proyecto y su difusión, con un el apoyo de la AMUE (encargada del desarrollo del software escolar que es un software a nivel nacional), RENATER, European Student Card y My Academic ID

- BCdiploma, una startup francesa especializada en credenciales digitales blockchain, ofrece una plataforma que permite a las instituciones emitir certificados digitales mediante una tecnología blockchain. El proyecto Fr.EBSI permitirá el despliegue de la solución BCdiploma en la Infraestructura de Servicios de Blockchain (EBSI) porque ahora está basada en el blockchain público Avalanche.

[10] Un "credential" es, por tanto, un documento que presenta información con referencias oficiales. La Verifiable Credentials es una versión digital de la credencial en la que toda la información es verificable porque se basa en tecnologías que garantizan su autenticidad.

- RENATER es la Red Nacional de Investigación y Educación se encarga del mantenimiento y pruebas de los nodos EBSI con sus socios GRnet, Belnet y RedIdriss.

Su funcionamiento:

Ilustración 5: El funcionamiento de BCdiploma según sus capas tecnológicas
Fuente: Esquema extraído del Libro Blanco de la Universidad de Lille, traducción propia

Está implementado en el blockchain Avalanche que funciona por Delegated Proof of Stake (DPoS) porque es más ecológico y rápido para hacer las transacciones, es decir, para añadir una información a un bloque. No se ha podido implementar en el EBSI todavía. La meta es dentro de un año implementarlo en el EBSI que es un blockchain de consorcio y funcionará con el PoA.

Las universidades tienen derecho a emitir los diplomas porque, en la mayoría de los casos, están acreditadas por el gobierno. Así, las universidades actúan como "Tercero de confianza" en este procedimiento garantizando que el diploma emitido para un alumno es veraz. La clave está en la confianza en las certificaciones, que sea el diploma de un trabajador que uno quiere en su empresa, que sea un producto en el supermercado con una certificación Bio que se quiere comprar. Damos importancia a las certificaciones por lo cual el tercero de confianza acreditado tendrá un papel preponderante asegurando la veracidad de la información antes de escribirla en el blockchain. Cada paso tiene su importancia.

Lo que se está poniendo en marcha es la certificación por el ministerio de educación superior de RENATER como nodo de confianza del EBSI. Este mismo ministerio ha acreditado las universidades francesas con un sello de calidad y confianza por lo cual

gracias a la cooperación de dichas entidades podrán en su momento emitir los diplomas de los alumnos en el EBSI.
Cuando llegue el momento de cambiar de tecnología blockchain, si nos fijamos en el esquema más arriba, se conservará la capa 3 y 4 y para implementarse en otra capa 1 y 2 que será el EBSI y funcionará con PoA para que no haya minado.

Su cumplimiento normativo:

La Universidad de Lille desarrolló una API para emitir los "verifiable credentials" junto a la plataforma BCdiploma encriptados en el blockchain Avalanche y BCdiploma genera un enlace por cada estudiante vinculado a su diploma. El enlace es personal, es propiedad del alumno que decide compartirlo (y en este caso expone datos personales como sería el caso de un diploma de papel fijado en una pared).
La base legal de este tratamiento es la obligación legal de la Universidad conservar los diplomas durante 50 años. Esta duración será el periodo de conservación de los datos para dicho tratamiento en el blockchain. En cuanto al típico problema del ejercicio de los derechos ARCOPOL[11], el derecho del estudiante a borrar sus datos no elimina la obligación de la universidad de emitir y archivar los diplomas (grados, másteres, etc). Se trata de un principio legal que ha permitido rechazar la solicitud de un estudiante de borrar su expediente. (Coëtlogon, 2022)

Conclusiones:

Digitalizar los diplomas se inscribe en los objetivos de Desarrollo Sostenible de la Agenda 2030 y en los acuerdos de París de 2015**,** reduce el papel, evita el desplazamiento de los alumnos hasta la Universidad para recibir su diploma al igual que evita encargar camiones para transportar dichos diplomas.
Luego, emitir un "Digital Credential" permite de una manera reducir el coste de los estudios, cuesta aproximadamente 2 euros contra 10 euros para un diploma en formato papel. La educación se financia con el dinero público, es decir, por los impuestos de todos los ciudadanos franceses por lo cual es un avance hacía la reducción de estos costes para

[11] El derecho de acceso, rectificación, supresión (cancelación), oposición, portabilidad, olvido y limitación del tratamiento

invertir este dinero en las infraestructuras, los profesores, etc. El EBSI promueve un modelo que permite un flujo fluido de intercambios entre el sistema de información de los ministerios y de las instituciones de enseñanza superior. Esto permitirá a las instituciones mantener un cierto nivel de autonomía en sus procedimientos, al tiempo que los armoniza a nivel nacional y europeo.

3.Blockchain aplicado para la mejora de la actividad económica a nivel local:

3.1. Panorama general

El autoconsumo aparece en la legislación de la UE en 2018 como parte del Paquete de Energía Limpia. La Directiva relativa al fomento del uso de energía procedente de fuentes renovables (DIRECTIVA UE 2018/2001) establece una definición de "autoconsumidores de energía renovable" en su artículo 2, 14) y una definición de "autoconsumidores de energía renovable que actúan colectivamente" en su artículo 2, 15).
Luego, el artículo 21 de la misma directiva introduce también la noción de "derecho al autoconsumo", que los Estados miembros deben garantizar a los consumidores.

Además, el artículo 15 de la Directiva 2019/944 sobre normas comunes para el mercado interior de la electricidad por la que se modifica la Directiva 2012/27/UE introduce la noción de **"cliente activo".** Señala que

> Los Estados miembros garantizarán que los clientes finales tengan derecho a actuar como clientes activos sin estar sujetos a requisitos técnicos o administrativos, procedimientos o gastos, desproporcionados o discriminatorios, ni a tarifas de acceso a la red que no reflejen los costes.

En la normativa francesa, la ley de 24 de febrero de 2017 relativa al autoconsumo incluyó en el código energético la definición de autoconsumo. Estas disposiciones fueron modificadas posteriormente por la ley sobre el crecimiento y la transformación de las empresas (conocida como ley "PACTE"), así como por la ley de 8 de noviembre de 2019 sobre energía y clima.

Para gestionar una operación de autoconsumo colectivo, la ley[12] creó un entorno sostenible para que suceda este modelo más ecológico y que comuniquen entre ellas las entidades que gestionaran los diferentes pasos del consumo y reparto de la energía producida, al igual que la tarificación aplicable para que las personas que producen su propia energía y la venden no soportan excesivos gastos o impuestos.
Es relevante constatar que la ley no prohíbe, pero tampoco incita textualmente su implementación en una estructura tipo blockchain.

Destacamos los siguientes artículos en el código de energía:

El artículo L.315-3 prevé la fijación de tarifas específicas para las operaciones de autoconsumo. Establece que

> la Comisión de Regulación de la Energía establecerá tarifas específicas para el uso de las redes públicas de distribución de electricidad para los consumidores que participen en operaciones de autoconsumo, tal y como se definen en los artículos L. 315-1 y L. 315-2, de modo que estos consumidores no estén sujetos a tarifas de acceso a la red que no reflejen los costes soportados por los operadores de la red.

El legislador impulsó el desarrollo de dichos modelos de economía colaborativa en 2017 pero en este momento no se mencionaba el blockchain, pero siguiendo la letra de la ley aparece ser una tecnología que ayudaría a implementar estos nuevos modelos de producción y consumo de energía.

El artículo L.315-6 pretende adaptar el actual marco técnico y contractual a las operaciones de autoconsumo:

> los gestores de la red pública de distribución de electricidad aplicarán las medidas técnicas y contractuales necesarias, en particular en lo que respecta a la medición de la electricidad, para permitir que las operaciones de autoconsumo se realicen en condiciones transparentes y no discriminatorias

[12] El Código de Energía y en especial las disposiciones relativas al autoconsumo

Entendemos aquí que el blockchain es relevante en este ámbito ya que permite cumplir con la ley para que las operaciones de autoconsumo se realicen de manera transparente.

3.2. Proyecto de autoconsumo colectivo DIGISOL con la startup SUNCHAIN, implementado en la región ROUSSILLON

Según el Real Decreto 244/2019 de 5 de abril, se entiende por autoconsumo colectivo cuando un grupo de consumidores se alimenta, de forma previamente acordada, de energía eléctrica que proviene de instalaciones de producción próximas al lugar en que se consumen y asociadas al mismo.

El departamento de los Pirineos Orientales, con sede en Perpiñán y cofinanciada por ADEME[13] en el marco del programa "Investissements d'Avenir", DIGISOL experimentó el autoconsumo colectivo entre 2017 y 2021. En este marco, la startup Sunchain está ayudando al Consejo Departamental del Roussillon (entidad pública) a definir la distribución de la producción entre los consumidores utilizando la tecnología Hyperledger, una red blockchain privada apoyada por la Fundación Linux. Opera en 2 ámbitos:

- El autoconsumo dentro de un edificio, en particular para las viviendas sociales;
- El autoconsumo entre edificios

Se tratan de redes virtuales entre productores y consumidores, utilizando los datos de los contadores de electricidad. La información sobre el consumo de los participantes está cifrada y almacenada en un blockchain. La distribución de la electricidad entre los participantes se realiza de forma automática y certificada según las condiciones infalsificables programadas en la cadena de bloques.

Ventajas para el consumidor:

[13] ADEME (Agencia de Medio Ambiente y Gestión de la Energía) es una institución pública de carácter industrial y comercial (EPIC) bajo la supervisión de los Ministerios de Transición Ecológica y Cohesión Territorial, Transición Energética y Enseñanza Superior e Investigación.

- ser un participante activo en su consumo de energía, sin tener que instalar paneles solares en su tejado
- reducir los costes energéticos

Ventajas para el productor:

- elegir la ubicación más adecuada para la instalación de paneles solares
- optar por una producción energética que tenga sentido

¿Por qué el blockchain y qué tipo de consensus elegido?

Primero para la seguridad de los datos, la robustez del sistema informático y, lo que es más importante, actúa como entidad de certificación autónoma y descentralizada. Los usuarios podrán tener mayor confianza en el tratamiento de sus datos.
Luego, tiene un gran potencial de exportación. Un sistema de este tipo puede reproducirse en todo el mundo. Francia tiene un único gestor de red para la mayor parte del país, pero no es así en todas partes. Un sistema basado en una cadena de bloques podría ser la interfaz de confianza para los proyectos interterritoriales.
Sunchain optó por un blockchain con permisos y un proceso de validación basado en una solución de PoS por la rapidez de sus transacciones y la preocupación medioambiental.

Así, Enedis ha interconectado sus sistemas con el blockchain para recoger el balance de los flujos de energía entre producción, exportación y consumición.

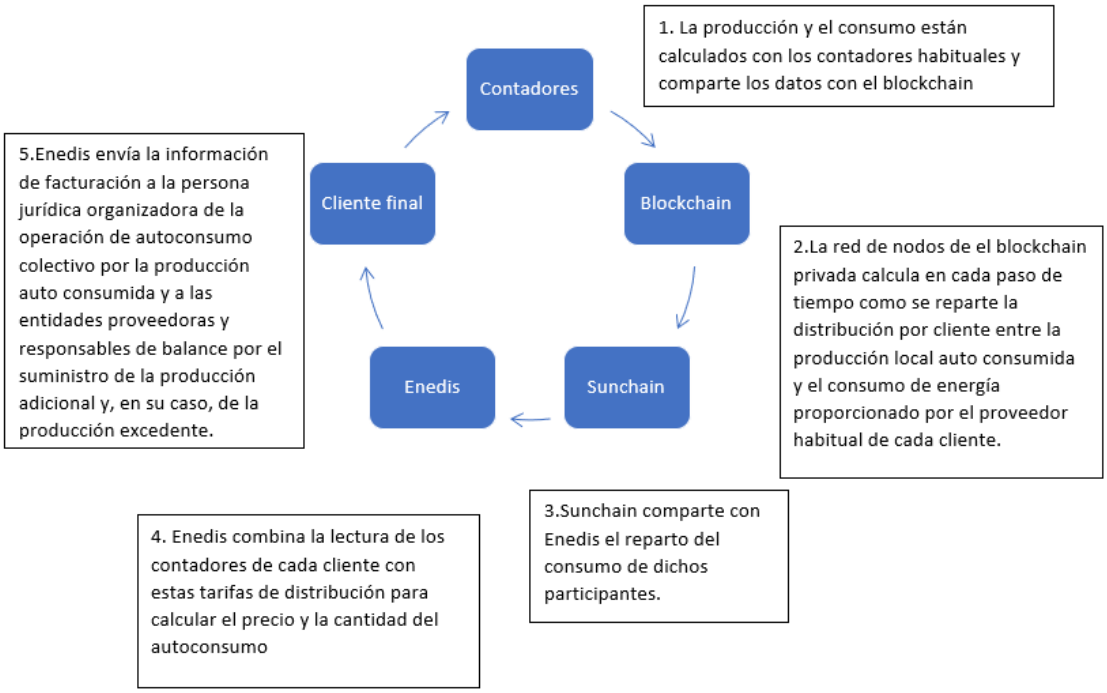

Ilustración 6: El funcionamiento de DIGISOL cronológicamente

Fuente: Información tomada de la empresa Sunchain
Diseño y traducción propios

Para los participantes y consumidores el proyecto DIGISOL permite:

- que se les asigne en cualquier momento su cuota de producción local calculada a través del protocolo de la cadena de bloques
- recibir suministro de electricidad, incluso en ausencia de producción, a través de la red pública de distribución
- valorizar los excedentes de producción no consumidos en la explotación
- acceder a datos fiables y seguros certificados por Enedis
- ser libre de elegir su proveedor de electricidad para la electricidad no autogenerada

III. Recomendaciones finales

El blockchain aparece como una herramienta para restaurar la confianza entre la Administración y las empresas con los ciudadanos porque los datos son distribuidos y no todos tendrán acceso a los datos en cualquier momento. Uno de los beneficios de esta herramienta es que puede contribuir en la protección al ciudadano y a sus datos

personales, sin embargo, por su carácter innovador conlleva a pensar en algunos momentos que se corresponde a una tecnología oscura asociada a las criptomonedas.

Por un lado, el blockchain sea público o privado permite a los ciudadanos tener un control efectivo sobre cómo se utilizan sus datos y a quién se le da permiso para acceder a ellos, esta mejora sobre el uso de los datos ha sido ilustrado por los casos de BCdiploma y de Agdatahub. Por otro lado, se identifica que para mejorar el bienestar local y fomentar la participación política, es más adecuado recurrir a un blockchain público. Se puede subrayar que son estas redes las que aportan en dichos escenarios democráticos atributos como la transparencia y la descentralización. Por cierto, los blockchains privados, aunque son menos disruptivos también aportan una respuesta a los problemas de transparencia. De hecho, una empresa o un ayuntamiento que usa una red privada blockchain conserva su estructura centralizada, pero mejora la trazabilidad y la inalterabilidad de las transacciones que ocurren entre los participantes como si fuese una base de datos inmutable. Digisol con la creación de un sistema de autoconsumo colectivo registrado en un blockchain ilustra un uso adecuado de un blockchain privado.

Para hacer buen uso de la tecnología blockchain por parte de las entidades públicas o por los prestadores privados a nivel local que tengan especial interés público, la clave reside en la elección del mecanismo de consenso. La Administración no puede pretender servir con objetividad los intereses generales que le corresponde según el artículo 103.1 de la Constitución Española si elige un mecanismo de PoW. Este mecanismo genera consecuencias negativas para el medio ambiente derivado de la potencia y volumen de cálculo de los mineros conllevando este hecho a un incumplimiento del acuerdo de París sobre el cambio climático ni los objetivos de desarrollo sostenible. Así, el uso del blockchain por parte de los ayuntamientos o empresas estudiados tiene un impacto significativo y novedoso cuando usan una red pública mientras se elige un mecanismo de consenso adecuado con el propósito final y, sobre todo, sin recurrir al mecanismo del PoW. El DPoS elegido por BCDiploma junto con la Universidad de Lille resulta ser un buen compromiso porque alcanza altos niveles de seguridad a través del algoritmo elegido para determinar los "Blockmakers" o validadores de bloques y también para verificar que los nodos son sean de alta calidad e individuos únicos.

Dentro de los casos estudiados, los proyectos con mayor impacto y viabilidad para mejorar el bienestar a nivel local son sobre los "Verifiable Credentials" y por

consecuencia, necesita la digitalización de los documentos físicos. Los proyectos de BCdiploma y Agdatahub son buenos ejemplos de este uso. Los "Verifiable Credentials" son muy prácticos porque al desmaterializar los diplomas, certificados y constancias optimiza el proceso administrativo y permite el acceso rápido e inmediato a los documentos y datos relacionados en cualquier momento y a raíz de las solicitudes de las empresas o administraciones. Con la tecnología blockchain es imposible modificar los documentos almacenados en ella, documentos que en cada caso han sido acreditados por un tercero de confianza como FranceConnect y el Ministerio de agricultura en el caso de Agdatahub, y por otro lado las Universidades ellas mismas acreditadas por el Ministerio de Educación Superior en el caso de BCdiploma. El riesgo residiría en el uso excesivo del "Verifiable Credentials". Esto llevaría en parte a la pérdida de confianza del uno en el otro, es decir, solo confiar en un justificante digital almacenado en el blockchain y no en la persona en sí, tampoco en sus certificados en papel porque pueden llegar a ser falsificados.

Cabe destacar que el proyecto "Neuilly Vote" es novedoso, al existir o presentarse escasez de proyectos piloto o experimentos sobre los votos en línea con el blockchain por varias razones. El precio alto de las transacciones restringe las iniciativas públicas porque se trata de dinero público, el propósito final no es aumentar los impuestos de los habitantes sino fomentar el interés en la toma de decisión. La inmediatez en la generación del resultado es el núcleo de una aplicación de voto en línea mientras que registrar una información en el blockchain no es inmediato, y costoso. Por estas razones, el uso de un blockchain para fomentar la participación política local no es al alcance de cualquier ayuntamiento, necesita dinero e instalaciones adaptadas en la ciudad para que cualquiera pueda votar en un dispositivo digital.

De cara al futuro, el EBSI podría ser una revolución para el sector público aprovechando la cooperación de diferentes entidades publicas en los países de la UE y por lo tanto llegando al consenso con un mecanismo ecológico, la PoA. El EBSI daría respuesta, por un lado, a los mínimos legales y técnicos requeridos en tema de seguridad de los sistemas informáticos de las entidades públicas por la robustez de su estructura, y por otro, mejoraría el control de los ciudadanos sobre sus datos personales gracias a la inmutabilidad, trazabilidad y transparencia del blockchain. Se entiende que se cumpliría el RGPD por la estructura en sí y los mecanismos criptográficos, aunque siempre se

deberá tener cuidado con los derechos ARCOPOL buscando una base legal en la que ampararse para que se respecte dichos derechos, como el derecho de supresión. Un buen ejemplo es BCdiploma porque cumple con todos los requisitos del RGPD al encontrar respuesta al derecho de supresión del artículo 17. Así, amparándose en la ley pudo afirmar que el derecho del estudiante a borrar sus datos no elimina la obligación de la universidad de emitir y archivar los diplomas.

En cuanto al marco normativo del blockchain, todavía tiene una definición legal muy limitada y ligada al sector financiero y a las criptomonedas, pero la novedad surgió en el sector energético. De hecho, esta tecnología da respuesta a la obligación de implementar medidas técnicas y contractuales para que se realicen las operaciones de autoconsumo colectivo en condiciones transparentes y no discriminatorias.

Ahora bien, en relación con los datos personales, se nota una elusión del cumplimiento del RGPD por ser tecnología novedosa y difícil de aprehender. En ciertos proyectos sus creadores o administradores, consideran que el dato almacenado en el blockchain no es un dato personal, pero al hacer una aproximación a las definiciones de las autoridades de protección de datos lleva a inferirse que los mimos pueden ser catalogados como datos personales.

Bibliografía

Libros:

De Filippi, P., & Wright, A. (2019). *Blockchain and the law, the rule of code*

NAKAMOTO, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*

Artículos:

Cárceles, M. P. (28 de marzo de 2019). La utilización del blockchain en los procedimientos de concurrencia competitiva. *Revista General de Derecho Administrativo*. Obtenido de https://laadministracionaldia.inap.es/noticia.asp?id=1509448

Morrow, M. J. (s.f.). The Promise of Blockchain and Safe Identity Storage for Refugees. Obtenido de https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/04/fs.pdf

Ponce de León. (2018). Blockchain, un nuevo patrón tecnológico. Thomson Reuters-Aranzadi.

Documentos electrónicos de organismos oficiales:

CNIL. (s.f.). *CNIL*. Obtenido de https://www.cnil.fr/fr/definition/blockchain#:~:text=La%20blockchain%20est%20une%20technologie,sans%20organe%20central%20de%20contr%C3%B4le.

Comisión Europea. (s.f.). Obtenido de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

EBSI. (s.f.). Obtenido de https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

Documentos oficiales:

de Coëtlogon, P., Durand, M., Jeantet, M., Génin, C., Ramon, R., & Boulet, P. (2021). Libro Blanco. *Les technologies blockchain au service du secteur public*. Obtenido de https://blockchain.univ-lille.fr/en/accueil/

Recursos de internet:

Accenture. (s.f.). Obtenido de https://www.accenture.com/be-en/services/blockchain/digital-identity

Accenture Technology. (13 de julio de 2018). Building A Trusted Identity: Blockchain ID Demo. Obtenido de https://www.youtube.com/watch?v=QYy8a7HDJ0g&t=62s

Agdatahub. (s.f.). Obtenido de https://agdatahub.eu/

BBVA. (3 de mayo de 2018). Obtenido de https://www.bbva.com/en/difference-dlt-blockchain/

BCDiploma. (s.f.). Obtenido de https://www.bcdiploma.com/fr

Binance Academy. (6 de Diciembre de 2018). *Binance Academy*. Recuperado el 08 de agosto de 2022, de https://academy.binance.com/es/articles/proof-of-work-explained

Bit2Me Academy. (s.f.). Obtenido de https://academy.bit2me.com/que-es-proof-of-authority-poa/

Bit2Me Academy. (s.f.). Obtenido de https://academy.bit2me.com/que-es-proof-of-stake-pos/

Bit2Me Academy. (s.f.). Obtenido de https://academy.bit2me.com/que-es-dpos/

Bit2Me Academy. (s.f.). *Bit2Me Academy*. Obtenido de https://academy.bit2me.com/que-es-un-ataque-del-51/

Brancato, R. (30 de junio de 2021). *RadioFrance*. Obtenido de https://www.radiofrance.fr/franceinter/a-neuilly-sur-seine-la-technologie-blockchain-pour-inciter-les-habitants-au-vote-electronique-3756292

Comben, C. (31 de may de 2020). *COINCENTRAL*. Obtenido de https://coincentral.com/blockchain-and-human-rights/#:~:text=Of%20the%2030%20articles%20on,illicit%20slavery%20and%20human%20trafficking

Digisol. (s.f.). Obtenido de https://www.digisol.com/

Dimitri Nitchoun y Bilal El Alamy. (12 de Agosto de 2019). *Equisafe*. Recuperado el agosto de 2022, de https://medium.com/@Equisafe/enfin-comprendre-la-diff%C3%A9rence-entre-blockchain-priv%C3%A9e-et-blockchain-publique-c9cf4eb003bd

elia. (s.f.). Obtenido de https://www.elia.be/en/news/press-releases/2018/08/20180823_press-release-elia-settlemint-actility-launch-first-blockchain-pilot-projects-energy-sector

Guillard, E. (22 de mayo de 2020). *Dexma Energy Intelligence*. Recuperado el 2022, de https://www.dexma.com/blog-en/the-disruptive-blockchain-technology-is-transforming-the-energy-sector/

IBM. (s.f.). Obtenido de https://www.ibm.com/case-studies/plasticbank

IBM. (s.f.). Obtenido de https://www.ibm.com/es-es/blockchain/solutions/food-trust

Izquierdo, E. (13 de junio de 2019). *cesnext*. Recuperado el 25 de agosto de 2022, de https://www.cesnext.com/noticias/i-voting-el-sistema-que-permite-votar-desde-casa-en-estonia/

jaimerueiljeparticipe. (s.f.). Obtenido de https://jaimerueiljeparticipe.fr/fr-FR/

Javier Gómez de Vera. (13 de junio de 2022). TFG - Servicios de participación ciudadana soportados en Blockchain. Obtenido de https://riull.ull.es/xmlui/bitstream/handle/915/28726/Servicios%20de%20participacion%20ciudadana%20soportados%20en%20Blockchain.pdf?sequence=1

Lyon Confluence. (s.f.). Obtenido de https://www.lyon-confluence.fr/fr/eureka-linnovation-au-service-du-bien-etre

MOBICHAIN. (s.f.). Obtenido de https://www.mobichain.eu/pourquoi-maas-4-0

MyDonor. (s.f.). Obtenido de https://mydonor.es/

Neuilly-sur-seine. (s.f.). Obtenido de https://www.neuillysurseine.fr/actualites/neuilly-annonce-la-creation-la-1ere-plateforme-municipale-vote-en-ligne

Orange Business Services. (s.f.). *YouTube*. Obtenido de https://www.youtube.com/watch?v=t__omVbgmEM

Think Smart Grids. (marzo de 2019). *Think Smart Grids*. Obtenido de https://www.thinksmartgrids.fr/actualites/blockchain-domaine-energie

Vignon, Q., & Mentré, G. (marzo de 2022). PODCAST- La Mairie, le podcast. *Tout comprendre sur le vote en ligne avec Gilles Mentré, co-fondateur d'Electis*.

von Blücher, U. (2022). *ComputerWeekly.es*. Obtenido de https://www.computerweekly.com/es/opinion/Fraude-digital-el-lado-oscuro-de-la-transformacion-digital-acelerada

Entrevistas:

Agdatahub, D. d. (Agosto de 2022).

Coëtlogon, P. d. (Agosto de 2022).

ANEXO I. Legislación estudiada

Comunitaria:

DIRECTIVA (UE) 2018/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 11 de diciembre de 2018 relativa al fomento del uso de energía procedente de fuentes renovables

DIRECTIVA (UE) 2019/944 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 5 de junio de 2019 sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Francesa:

Code de l'énergie (Código de energía francés)

Code monétaire et financier (Código de Comercio francés)

Decreto nº2018-1226 de 24 de diciembre de 2018, sobre la utilización de un dispositivo de registro electrónico compartido para la representación y transmisión de valores financieros y para la emisión y transferencia de "miniobligaciones".

Ley del 24 de febrero de 2017 relativa al autoconsumo

Ley "PACTE" sobre el crecimiento y la transformación de las empresas

Orden de 8 de diciembre de 2017 sobre el uso de un dispositivo de registro electrónico compartido para la representación y transmisión de valores financieros.

Española:

Constitución española

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

ANEXO II: Entrevista con Agdatahub sobre su SaaS Agriconsent

1. ¿Cuáles son los beneficios para los consumidores y clientes de este agricultor? ¿Podemos ver la trazabilidad de los alimentos que compramos a este agricultor (o incluso en el supermercado si los productos proceden de su granja, por ejemplo)? ¿Hasta qué punto este innovador sistema puede beneficiar a la comunidad agrícola al autentificar sus documentos, pero sobre todo al resto de la sociedad?

En su primera versión, esta herramienta está destinada al agricultor. La principal ventaja es que podrá identificarse con un nivel de seguridad extremadamente alto muy rápidamente. Esto mejorará su carga de trabajo y su comodidad laboral, lo que mejorará toda la cadena de valor de la producción agrícola.

Además, permitirá un control rápido y fiable de los distintos certificados concedidos a la persona física o jurídica (certificado de autorización de uso de productos fitosanitarios, certificado de agricultura ecológica, etc.), lo que beneficiará al resto de la empresa.

Por otro lado, esta herramienta no está pensada para rastrear la producción (existen muchos otros proyectos para ello, por ejemplo, la cadena de cristal).

2. Cuando/antes de implementar los certificados de identidad de un agricultor a la cadena de bloques, ¿quién se encarga de comprobar que estos documentos son legales? ¿Existe un tercero (persona física) que sea de "confianza" y esté detrás de estas verificaciones?

La herramienta permitirá gestionar las identidades, o más exactamente los "Verifiable credentials". Sólo se registran en el blockchain las pruebas de entrega de estos atributos, no la información que los compone (nombre, apellido, razón social, etc.). Estos últimos sólo se almacenan en la aplicación instalada en el teléfono móvil del agricultor, que por tanto tiene el control de su información personal.

Las pruebas de entrega de los certificados están "firmadas" por las autoridades competentes, según el certificado (por ejemplo: el Ministerio de Agricultura francés a través de las cámaras de agricultura para los certificados de identidad de las personas físicas y su vínculo con la identidad de las personas jurídicas)

3. ¿Qué tipo de blockchain (pública/privada/mixta) utiliza y por qué ha hecho esta elección?

Se trata de un blockchain de consorcio para que el acceso esté limitado a los actores de confianza

4. ¿Cómo se gestiona la ciberseguridad, quién accede a la cadena de bloques y cómo? En otras palabras, si se trata de un blockchain privado, ¿cómo se eligen las personas encargadas de aceptar la creación de un nuevo bloque en la blockchain?

Los actores que tienen acceso a la cadena de bloques se identifican para cumplir con el acuerdo entre agdatahub y el Ministerio de Agricultura francés

5. ¿Cómo gestionar la eficiencia energética? Dado que la tecnología blockchain consume mucha energía, ¿hay algo que podamos hacer al respecto?

El blockchain utilizado (alastria) no utiliza la prueba de trabajo utilizada en las criptomonedas y, por lo tanto, consume relativamente poca energía

6. Por definición, el blockchain es un protocolo descentralizado, lo que dificulta la designación de responsable de tratamiento

No se procesa información personal en la cadena de bloques, por lo que no hay responsable de tratamiento