BLOCKCHAIN Y ADMINISTRACIONES PÚBLICAS:

La Tecnología Blockchain en la Administración Pública: Aplicaciones y Prueba de Concepto

Indice

1.- INTRODUCCION

Objetivo:

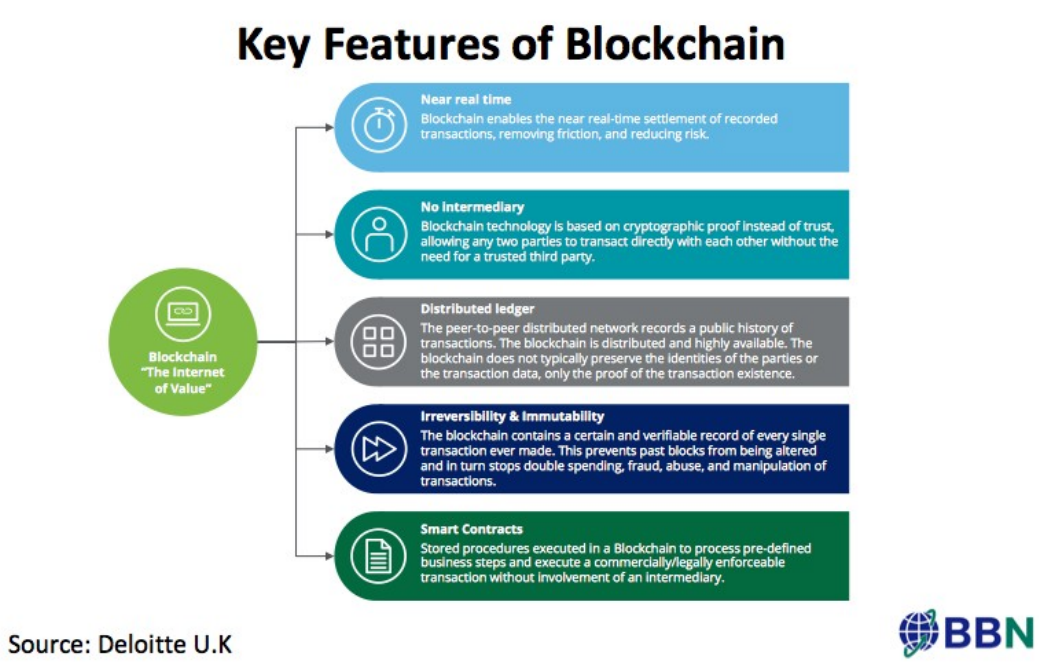
Uno de nuestros objetivos, es el de profundizar en las tecnologías blockchain y en sus aplicaciones prácticas en los distintos ámbitos sociales y en este caso, dentro de los canales de comunicación entre el Ayuntamiento de Madrid y sus conciudadanos.

Como objetivo ulterior, y mas a largo plazo es crear un prototipo de aplicación que pueda integrarse como una capa añadida al sistema informático de gestión Linea Madrid, en el ámbito que se determine y sin que afecte al normal funcionamiento del mismo. Este prototipo añadirá las ventajas que ofrece el uso de los sistemas de bases de datos distribuidas, tecnología conocida como blockchain, entre las que cabe destacar la imposibilidad de modificar los datos una vez incluidos y procesados en la cadena de información, con las ventajas consiguientes en cuanto a transparencia y en su caso, preservación de la intimidad del consultante.

Los negocios, el gobierno y la sociedad están basados en la confianza. Por eso muchas personas todavía se muestran escépticas al oír hablar de una tecnología que promete transformar el modo en que la logramos y aplicamos.

¿Que es la tecnologia Blockchain?

Blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. También se puede definir como una base de datos compartida que funciona como un libro de registro de operaciones de compra y venta, como los libros contables.



Básicamente, el blockchain funciona como un libro de contabilidad muy complejo: proporciona una estructura de datos a prueba de falsificaciones que permite identificar la identidad en origen y destino durante una transacción, verificar que es auténtica y dar el visto bueno para que se realice, de forma que cada cadena de datos criptográficos que verifica una transacción sea imposible de replicar, y por tanto, de falsificar. Y lo más importante: la registra para la posteridad.

A día de hoy, las transacciones realizadas con Bitcoin están secuenciadas a través de blockchain utilizando sistemas de cifrado SHA-256, de forma que todas las trasacciones que se hacen a través de esta base de datos distribuida son firmadas mediante una clave privada a prueba de manipulaciones por terceros.

Bienes digitales y Monedas Digitales

Para entender mejor lo que estamos exponiendo en este documento, necesitamos entender los dos conceptos:

El bien digital es un servicio de software, al que puede accederse remotamente, sin intervención humana, y cuyo contenido es universal (sonido, imagen, datos, hechos) transmitidos electrónicamente, que puede disfrutarse o utilizarse previo derecho de acceso u uso, oneroso o gratuito, que no tiene equivalencia o simetría con el bien material o físico que representa, salvo por aproximación.

La moneda digital es más que un bien digital en sentido estricto: un bien de información intangible fundado en protocolos especificos de software libre, representativo de un bien fisico o material(por ejemplo, dinero) y , detalle significativo, en el que la creación de moneda da lugar a contraprestación por el trabajo realizado por determinado usuario o partícipe (miner) en la comunidad en red.

Internet de la Informacion vs Internet del Valor

Blockchain, dicen los expertos, va a posibilitar dar el salto del llamado *internet de la información* al *internet del valor*. Durante los últimos 23 años hemos convivido con el primero, un ecosistema que ha penetrado hasta las profundidades de nuestro día a día y que ha hecho que florezcan empresas como Google, Facebook o Twitter. Estos nombres han cambiado modelos de negocio de industrias enteras como los medios de comunicación, las telecomunicaciones o el turismo.

Se le llama internet de la información porque hasta ahora lo que se ha compartido ha sido fundamentalmente información. Ahora, estamos dando el salto hacia el *internet del valor*. Y esta ola es mucho mayor que la primera

Realmente el Internet del valor, es una infraestructura que te permite construir sobre internet, y crear otra capa sobre la que las personas van a poder intercambiar valor entre ellas". Eso afecta a todos los sectores: ya tocó a la banca, pero va a afectar también al sector de las energías, a las telecomunicaciones, a las cadenas de valor de logística, etc. etc.

Internet del valor : Salto Tecnologico y social

El mundo cambió de repente, de forma repentina, sin que muchos vieran el impacto real que iba a tener en el futuro y que tendrá, fue con la aparición de los bits, no hablemos técnicamente de lo que son los bits, sino intentar transmitir el concepto de digitalización. Hoy en día, todo se puede almacenar, todo deja huellas digitales, hay suficiente capacidad como para almacenar toda la información generada por el hombre durante los últimos 40.000 años.

“mientras los sistemas sociales cambian incrementalmente, la tecnología lo hace de forma exponencial, creándose así una brecha que posibilita los cambios discontinuos y revolucionarios”.

Estamos viviendo una época interesante, las antiguas estructuras esclerotizadas, pueden provocar la aparición de fuerzas de transformación y de regeneración que cambian el paradigma de ciertos sectores de una forma tan radical que cuesta imaginarlo.

Hasta ahora, las organizaciones han tenido que adaptarse y adoptar los beneficios que ha creado la era digital, han tenido que rediseñar sus diferentes sistemas de comunicación internos para introducir ordenadores y software necesarios para facilitar tareas y operaciones que se llevan a cabo dentro de ellas o mínimo en sus principales áreas.

Pero con blockchain las posibilidades de transmitir informacion de bienes digitales y que todo el mundo pueda intercambiar y compartir valor de igual a

igual(P2P) mediante criptomonedas propias, nos deja claro que el poder no va a estar tan centralizado. Eso cambia la operativa de las empresas, pero también la operativa de las personas, cómo interactuamos ahora entre nosotros. Y esto es realmente fascinante, tratar de imaginar cómo va a ser el futuro en 20, 30 sobre todo a nivel social.

Lo cierto, es que hasta ahora aunque no de forma completa, las TIC habian resultado imprescindibles en aspectos de tanta repercusión social, como son la igualdad de oportunidades, la democratización en el acceso a la información, o la eliminación de los riesgos de las brechas socioeconómicos y culturales por motivos geográficos, de edad, de género, de origen, etc…

Blockchain puede provocar cambios profundos en todos estos casos, dentro de muy poco tiempo. Quizás uno de los efectos más interesantes de la economía descentralizada basada en protocolos abiertos: la redistribución del valor en esta transición.

Origen de de la tecnologia Blockchain: Criptoanarquía (Cipherpunk)

Los movimientos *cyberpunk*, *cypherpunk* y *hacktivista* sentaron las bases que permitirían crear la primera criptomoneda del mundo, el *bitcoin*; pero, más relevante aun, facilitaron idear el protocolo de cadenas de bloques, basado en la criptografia de clave publica, que habia nacido años antes, rompiendo la hegemonia de la NSA americana, basada en criptografia de clave privada simetrica

David Chaum es uno de los iniciadores de la criptografía aplicada a los pagos, firmas ciegas para pagos ilocalizables, imposibles de rastrear. Un sistema que, por un lado, no permite a terceras partes la determinación del perceptor, el tiempo o el importe de los pagos hechos por otra persona; importante en términos de intimidad y privacidad; por otra, la capacidad de los individuos para proveer una prueba del pago o informar de la identidad del perceptor bajo circunstancias excepcionales.

Entre 1992 y 1994 se difunde la criptografía como manifestación de un movimiento denominado criptoanarquÍa: un medio para tutelar la privacidad y la libertad individual en la red: “…*una criptografía potente puede causar la declinación del poder del estado y quizá aún colapsarlo. Creemos que la expansión en el ciberespacio con comunicaciones seguras, anonimato y seudónimos y otras interacciones criptomediales cambiaran profundamente la naturaleza de las interacciones económicas y sociales*.

“*La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el Nombre Auténtico, o la identidad*

legal, de la otra. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re-enrutado de paquetes encriptados en máquinas a prueba de manipulacion que implementen protocolos Criptograficos, con garantias casi perfectas, contra cualquier intento de alteracion.
Las reputaciones tendrán una importancia crucial, mucho más importante en los tratos que las calificaciones crediticias de hoy en dia. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar y de controlar las interacciones económicas, la capacidad de mantener la información secreta, e incluso alterarán la naturaleza de la confianza y de la reputación"

Timothy C.May Cifernomicron. Manifiesto

Tipos de Blockchain: Público, Privado e Híbrido

Existen tres tipos:

-Públicas

-Privadas

-Híbridas.

Blockchains públicas

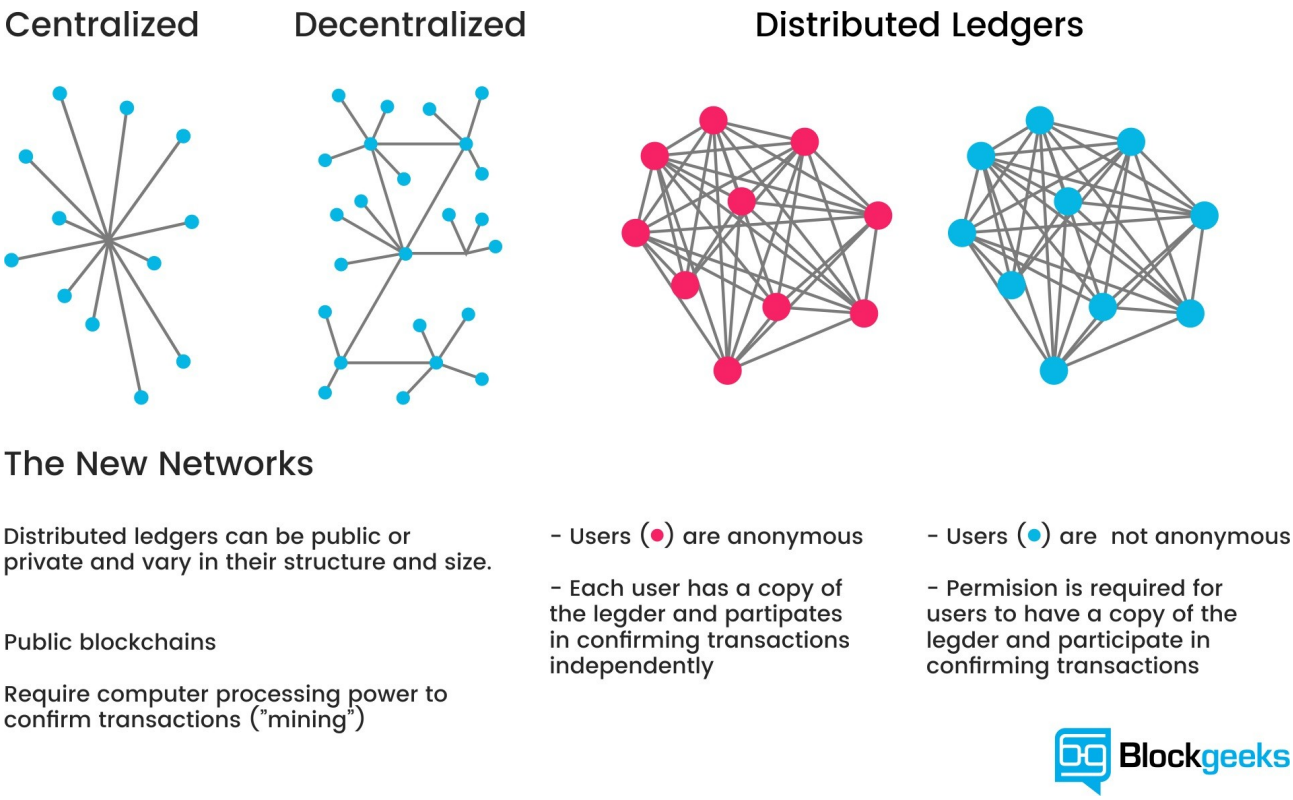
Los ejemplos más conocidos de Blockchains públicas son **Bitcoin y Ethereum.** Una Blockchain pública es accesible a cualquier usuario en el mundo. Lo único que se necesita es un ordenador y una conexión a Internet.

Ejemplo: Bitcoin

La Blockchain pública de Bitcoin se compone del *protocolo Bitcoin* (con B mayúscula), la unidad de cuenta o token bitcoin (con b minúscula) y la red blockchain (la base de datos en la que se registran las transacciones). Bitcoin ha sido el inventor del concepto Blockchain, inspirándose en otras soluciones y combinándolas de tal forma que se pudiera crear un sistema descentralizado que resolvía el problema del "doble gasto". El problema del "doble gasto", que se llevaba investigando por científicos en todo el mundo desde hace más de 30 años, decía que en un sistema descentralizado era imposible evitar que un activo o bien digital se gastará dos o más veces.

En un sistema centralizado evitar el problema del "doble gasto" es muy sencillo, pero en un sistema descentralizado en el que todos los ordenadores tienen una copia de todas las transacciones (la blockchain) la cuestión de cómo se ponen de acuerdo todos los nodos para definir cuál es la realidad de esa base de datos de forma descentralizada para llegar a un consenso y funcionar es un problema altamente complejo que nadie consiguió resolver hasta que apareció Bitcoin. Bitcoin resuelve este problema con las matemáticas, la criptografía y la comunidad Bitcoin (los usuarios, mineros, casas de cambio y

desarrolladores del ecosistema Bitcoin).



Blockchains privadas

Una Blockchain privada**,** a diferencia de una Blockchain pública, no está abierta al público, sino que solo se puede acceder a ella por invitación. Las Blockchains privadas son más nuevas que las Blockchains públicas y pueden ser muy diferentes las unas a las otras y en algunos casos es incluso cuestionable que se pueda hablar de Blockchain para algunas de las soluciones que se conocen en el mercado. Algunas de las más famosas son Hyperledger (de la Fundación Linux), R3 (un consorcio de bancos internacionales para desarrollar soluciones bancarias de blockchain privada) o Ripple (un protocolo para facilitar las transferencias internacionales de dinero).

Blockchains híbridas

Las Blockchain híbridas son una combinación de las públicas y privadas. En una Blockchain híbrida los nodos participantes son invitados, pero todas las transacciones son públicas. Eso quiere decir que los nodos participan en el mantenimiento y seguridad de esta blockchain, pero que todas las transacciones son visibles para usuarios en todo el mundo y que no tienen que conocer el contenido de la blockchain, a diferencia de las blockchains privadas

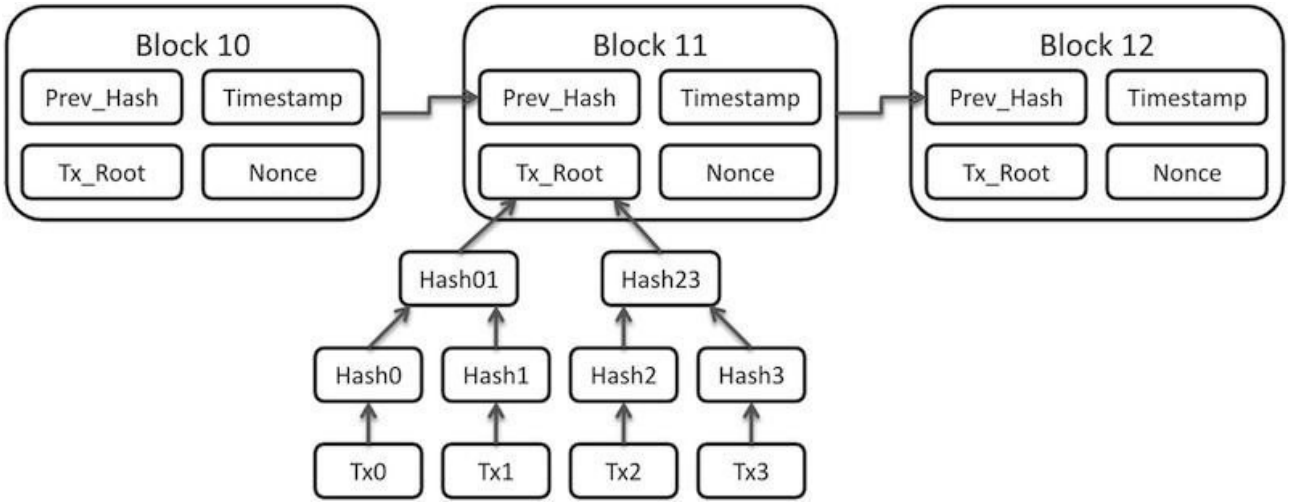
en la cual las transacciones son privadas también. Algunos ejemplos de blockchains híbridas son BigchainDB (un proveedor de tecnología Blockchain) o Evernym, una blockchain híbrida que quiere facilitar la gestión de la Identidad Digital Soberana (ltSelf Sovereign Identity).

2.- SISTEMAS BLOCKCHAIN PUBLICOS

Bitcoin con mas detalle:

Ya hemos explicado en parte Bitcoin anteriormente, como el gran ejemplo actual de Blockchain Publica.

Bitcoin es realmente, un conjunto de conceptos y tecnologías que conforman un ecosistema de dinero digital. El almacenamiento y transmisión de valor entre los participantes de la red bitcoin se consigue mediante la utilización de las unidades monetarias llamadas bitcoins. Los usuarios de bitcoin se comunican entre ellos usando el protocolo Bitcoin, principalmente a través de Internet, aunque también se pueden utilizar otras redes de transporte. La pila de protocolos bitcoin, disponible como software open source, puede ejecutarse sobre una amplia variedad de dispositivos, incluyendo Portatiles y smartphones, lo que hace que la tecnología sea fácilmente accesible.



Arbol de Hashes

Los usuarios pueden transferir bitcoins a través de la red para hacer prácticamente cualquier cosa realizable con monedas convencionales, incluyendo comprar y vender bienes, enviar dinero a personas y organizaciones, o extender créditos. Los bitcoins pueden comprarse, venderse e intercambiarse por otras monedas en casas de cambio especializadas. En cierta forma bitcoin es la forma de dinero perfecta para Internet, ya que es rápido, seguro y carente de fronteras.

Bitcoin es un sistema entre pares (peer-to-peer) distribuido. Como tal no existe ningún servidor o punto de control "central". Los bitcoins se crean mediante un proceso llamado "minería," que se basa en una competencia por encontrar

soluciones a un problema matemático a la vez que se procesan transacciones bitcoin. Cualquier participante de la red bitcoin (léase, cualquier persona utilizando un dispositivo con la pila de protocolos bitcoin completa) puede operar como minero, utilizando el poder de computacion de su computador para verificar y registrar transacciones.

Cada 10 minutos en promedio alguien consigue validar las transacciones de los últimos 10 minutos y es recompensado con nuevos bitcoins.
En esencia, la minería de bitcoins descentraliza la función de emisión de moneda y la autorización de un banco central, y reemplaza la necesidad de un banco central con esta competencia global.

El protocolo bitcoin incluye algoritmos que regulan la función de minería en toda la red. La dificultad de la tarea de procesamiento que los mineros deben ejecutar (para registrar con éxito un bloque de transacciones para la red bitcoin) se ajusta dinámicamente de forma que, en promedio, alguien tendrá exito cada 10 minutos sin importar cuántos mineros (y CPUs) hayan trabajado en la tarea en cada momento. Cada cuatro años, el protocolo también reduce a la mitad la tasa a la que se crean nuevos bitcoins, asegurando se seguirán creando bitcoins hasta un valor límite de 21 millones de monedas.

El resultado es que el número de bitcoins en circulación sigue de cerca una curva fácilmente predecible que alcanza los 21 millones en el año 2140. Debido a la decreciente tasa de emisión, bitcoin es deflacionario en el largo plazo. Además bitcoin no puede ser inflado a través de la "impresión" de nuevo dinero por encima de la tasa de emisión esperada.

Lo relevante: Revolucion en Computación Distribuida

Bitcoin da una solución a un Problema de Computación Distribuida, La invención de Satoshi Nakamoto es también una solución a un problema previamente sin solución en computación distribuida, conocido como el "Problema de los Generales Bizantinos."

Brevemente, el problema consiste en tratar de llegar a un consenso al respecto de un plan de acción intercambiando información a través de una red poco fiable y potencialmente comprometida.

La solución de Satoshi Nakamoto, que utiliza el concepto de prueba de trabajo para alcanzar un consenso sin requerir confianza en una autoridad central, representa un avance en computación distribuida y posee amplias aplicaciones más allá de las monedas. Puede ser utilizada para alcanzar consenso en redes distribuidas para probar la legitimidad de elecciones, loterías, registros de activos, autorizaciones bajo notario digitales, y más.

Ethereum: supercomputacion descentralizada

Imagina que toda la humanidad podría tener acceso a una sola super-computadora. Pero eso, de hecho, fue hecho de una combinación de cientos de miles de ordenadores, dispersas por el mundo, trabajando en la misma red, de manera descentralizada y procesando la misma información. Esta es básicamente la propuesta detrás de la plataforma Ethereum.

Ethereum es una plataforma digital cuya principal misión es la implementación de aplicaciones descentralizadas (dapps) y contratos inteligentes. “Dapps” son programas informáticos que eliminan la necesidad de intermediarios en virtualmente cualquier servicio centralizado existente al permitir que cualquiera confíe en una contraparte desconocida para realizar los más variados tipos de acuerdos y acuerdos de una manera 100% digital.

En Ethereum, los desarrolladores también pueden escribir lógica de negocio y acuerdos en forma de contratos inteligentes, los cuales se ejecutan automáticamente cuando sus condiciones son satisfechas por ambas partes e informadas a la red.

Estos contratos pueden almacenar datos, enviar y recibir transacciones e incluso interactuar con otros contratos, independientemente de cualquier control.

Inicialmente, el término "contrato inteligente" se utilizó para describir el uso de sistemas informáticos (u otros medios automatizados) que tenían por objeto realizar ciertos acuerdos.

ETHEREUM

UNA GUÍA INTRODUCTORIA

1 INTRODUCCIÓN

A lo largo de los últimos años, algunos desarrolladores han comenzado a utilizar la tecnología subyacente en el Bitcoin - La Cadena de Bloques - para crear nuevas y novedosas aplicaciones. Ethereum es una plataforma de próxima generación que permite que quienquiera - tanto desarrolladores como consumidores - pueda fácilmente tomar ventaja de redes descentralizadas y los beneficios de la tecnología de cadena de bloques.

2 Qué son redes descentralizadas?

Las redes descentralizadas redistribuyen las funciones y poderes, alejándolos de un servidor centralizado y permitiendo comunicación e interacción entre pares (p2p).

BitTorrent, usado para compartir archivos es un ejemplo de una red descentralizada.

3 La cadena de bloques

La mayoría de las redes funcionan usando una autoridad central para la toma de decisiones. La cadena de bloques, una especie de red descentralizada, puede lograr acuerdos a través de toda la red sin usar ninguna autoridad central.

Bitcoin usa la tecnología de cadena de bloques para registrar y verificar transacciones sin la necesidad de un banco central.

4 ETHEREUM

La visión de Ethereum es descentralizar el internet al crear una plataforma en la que las aplicaciones se crean y corren en una red descentralizada. Ethereum es rápido y flexible sin tener las limitaciones inherentes del protocolo de Bitcoin.

> **Lo que Bitcoin hace para transacciones financieras, Ethereum lo hace para cualquier cosa que puede ser programado**

5 ETHER

Ether es la ficha de cambio de Ethereum, y tiene dos propósitos. Primeramente, al requerir que las aplicaciones paguen Ether por cada operación que realizan, se previene que los programas rotos o maliciosos se salgan de control. En segundo lugar, se otorga ether como recompensa a quienes contribuyen con sus recursos a la red descentralizada.

Ether: El combustible que utiliza la red de Ethereum

6 MIST

Mist será la interfaz de usuario de Ethereum que llevará la tecnología de la cadena de bloques a los usuarios no técnicos.

Incluirá un catálogo de aplicaciones descentralizadas y una variedad de otras herramientas.

Mist funcionará de manera similar a las tiendas de aplicaciones y los navegadores a los que ya estamos acostumbrados

7 Para qué será usado Ethereum?

Los servicios que tradicionalmente son centralizados, pueden ser descentralizados usando Ethereum. Esto llevará a una reducción costos y comisiones al conectar a los individuos directamente y eliminando la necesidad de terceros.

Imagina servicios como Uber o eBay sin una empresa en el medio cobrando comisiones!

Usando Ethereum, IBM y Samsung trabajaron en una máquina lavadora conceptual, la cual podía:

- comprar su propio detergente cuando se le acababa
- llamar a su propio técnico cuando se decomponía
- lavar ropa a horas en las que la electricidad es más barata!

Los creadores del internet no se imaginaron las redes sociales o la nube. No tenemos manera alguna de predecir cuál tecnología innovadora nacerá de la cadena de bloques de Ethereum!

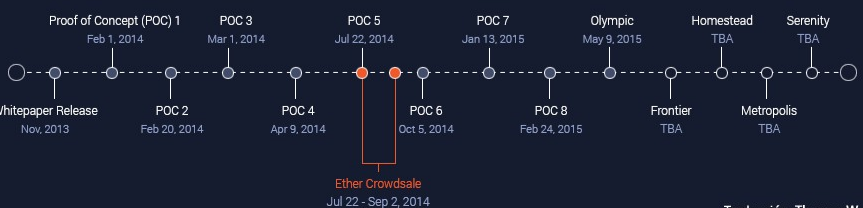
8 Qué se está construyendo ahora?

WeiFund	Plataforma de microfinanciación colectiva.
airlock	Protocolo de acceso para propiedades inteligentes y el Internet de Cosas.
PROVENANCE	Proyecto para mejorar la transparencia y rendición de cuentas de cadenas de proveedores
augur	Plataforma descentralizada de predicción de mercados.

9 Financiando la visión

El 22 de Julio de 2014, la organización sin fines de lucro Ethereum, lanzó una venta pública de Ether. Los fondos recolectados han ayudado a llevar adelante el desarrollo del proyecto. La venta duró 42 días y recaudó 31.591 BTC, o $18.439.086, haciéndolo el proyecto con la mayor financiación colectiva para la fecha.

42 Días	31 Mil BTC recolectados	$18 Millones
3rd Proyecto con mayor financiación colectiva a la fecha actual		9 Mil participantes



Traducción: Thomas W

Como ejemplo de un contrato mecánico inteligente, podemos mencionar una máquina que vende refrescos o chocolates. Cuando colocas un billete o moneda en estas máquinas, un sistema informático programado para identificar la cantidad recibida y el producto elegido hace cumplir un acuerdo entre el consumidor y el propietario de la máquina, realizando una venta automática.

Los dapps y los contratos inteligentes trabajan en el blockchain Ethereum, que tuvo su arquitectura inicial concebida por un joven genio ruso a la edad de 19 años, llamado Vitalik Buterin, quien eligió el siguiente título para su libro blanco: "*Ethereum: A Platform of Smart contracts and next generation decentralized applications*."

Una aplicación futura de Ethereum son DAOs o Organizaciones Autónomas Descentralizadas.

Un **DAO** se compone de uno o más contratos y podría ser financiado por un grupo de personas con ideas similares. Un DAO opera completamente transparente e independiente de cualquier intervención humana, incluyendo a sus creadores originales. Un DAO permanecerá en la red mientras cubra sus costos de supervivencia y proporcione un servicio útil a su base de clientes.

(Mas informacion de DAO en la seccion de Gobernanza del Capitulo 3)

Contratos inteligentes (Smart Contracts)

Realmente, se trata de meros programas de software que recogen los términos de un contrato entre las partes y se almacenan en la *blockchain*, con la peculiaridad de que se autoejecutan cuando se cumplen una serie de condiciones especificadas en el propio contrato.

De este modo se evitan los intermediarios, aligerando costes y retrasos burocráticos; así como cualquier tipo de interferencia por parte de un tercero.
Las posibilidades de esta funcionalidad combinada con otras nuevas tecnologías como el Internet de las cosas y las tecnologías financieras son enormes

Son contratos con las siguientes características:

- No requiere de intermediarios que lo validen o que garanticen su cumplimiento.
- No son interpretables, por o que evitas que alguno de los firmantes evite cumplir su parte del acuerdo en base a una interpretación subjetiva.
- Se cumple por sí mismo y se ejecuta cuando se cumplen las condiciones pactadas.
- Puede ser firmado por personas (físicas o jurídicas) o por máquinas

autónomas.
- y tiene todas las características inherentes al *Blockchain*: público, descentralizado, transparente e inmutable.

NOTA: Etherium de forma detallada en Repositorio MediaLab:

https://github.com/medialab-prado/blockchainapp/blob/master/Ethereum-intro.pdf

3.- TRANSPARENCIA Y EJEMPLOS DE USO DE BLOCKCHAIN EN LA ADMINISTRACION PUBLICA

Transparencia y El Derecho a la Información

Se reconoce el derecho a conocer datos e información sobre el funcionamiento económico del Estado, vinculado a su gestión administrativa y política. (Excluyendo de este apartado aquellas cuestiones de seguridad nacional.)

Este tipo de derechos tiene como única intención, verificar la correcta gestión de los fondos públicos de la Gestión Pública y de los políticos en el ejercicio de sus funciones institucionales.

Áreas de aplicación según la legislación Española:

Información Institucional:

- Organismos públicos
- Organigramas de departamentos, funciones y funcionarios
- Planes y Objetivos (estados de su cumplimiento)
- Retribuciones de Altos cargos y sus Curriculums
- Relaciones del puesto de trabajo por organismo: funcionarios, personal laboral, contrataciones y evolución.

Información Normativa y Jurídica:

- Normativa y legislación destacable
- Normativa vinculante a cada organismo público.
- Normativa y leyes en vigor
- Otras disposiciones.

Información Económica: Contratos; Convenios; Subvenciones; Patrimonio:

- Contrataciones y Contratos en vigor (información y seguimiento)
- Convenios y encomiendas
- Patrimonio y bienes Inmuebles vinculados a cada institución.

Información Presupuestos, Fiscalización e Informes:

- Presupuestos aprobados por Institución.
- Cumplimiento del Gasto, por Institución.
- Auditorías ejercicios anteriores.
- Información y estadísticas de interés (Open Data)

Es obligación de la Administración Pública asumir, de mantener actualizada de manera permanente y eficiente la información de su gestión pública a través de los Portales de Transparencia. Siendo estas sedes electrónicas lo puntos en los que han de converger toda la información de manera ordenada, legible, y fehaciente

Estado del cumplimiento de la transparencia de la Información en EUROPA:

En los últimos años se ha asistido a la demanda generalizada de mayores niveles de transparencia en la Unión Europea, aumentada por el impacto de la reciente crisis económica y el afloramiento de numerosos casos de corrupción. El derecho de acceso a la información es una de las piezas clave para el fortalecimiento de una cultura de la transparencia y que sirva para facilitar la participación de la ciudadanía en los asuntos públicos.

Este derecho ha experimentado una evolución en los últimos años, cuyo balance puede considerarse, en términos generales, como positivo. Además de su reconocimiento por el derecho originario de los Tratados, cabe destacar el Reglamento 1049/2011, que se encuentra actualmente en proceso de reforma.

Conviene resaltar también la labor de la jurisprudencia en la materia tanto del Tribunal de Justicia de la Unión Europea, como del Tribunal Europeo de Derechos Humanos, que han contribuido a delimitar el alcance del derecho de acceso a la información y documentos comunitarios. En este sentido, en el año

2009 tuvieron lugar dos sentencias de suma importancia en el TEDH, que contribuyeron a marcar un punto de inflexión para considerar el derecho de acceso como derecho fundamental y quedar amparado por la Convención Europea de Derechos Humanos. Este hecho coincide en el tiempo con la adquisición de fuerza vinculante de la Carta de Derechos Fundamentales de la Unión Europea, que reconoce el derecho de acceso en su articulado.

Pese a estos avances, la UE sigue enfrentándose a nuevos retos en un momento en el que la transparencia, la participación ciudadana, el buen gobierno y el derecho de acceso a los documentos públicos se han convertido en piedras angulares del funcionamiento democrático de las sociedades avanzadas.

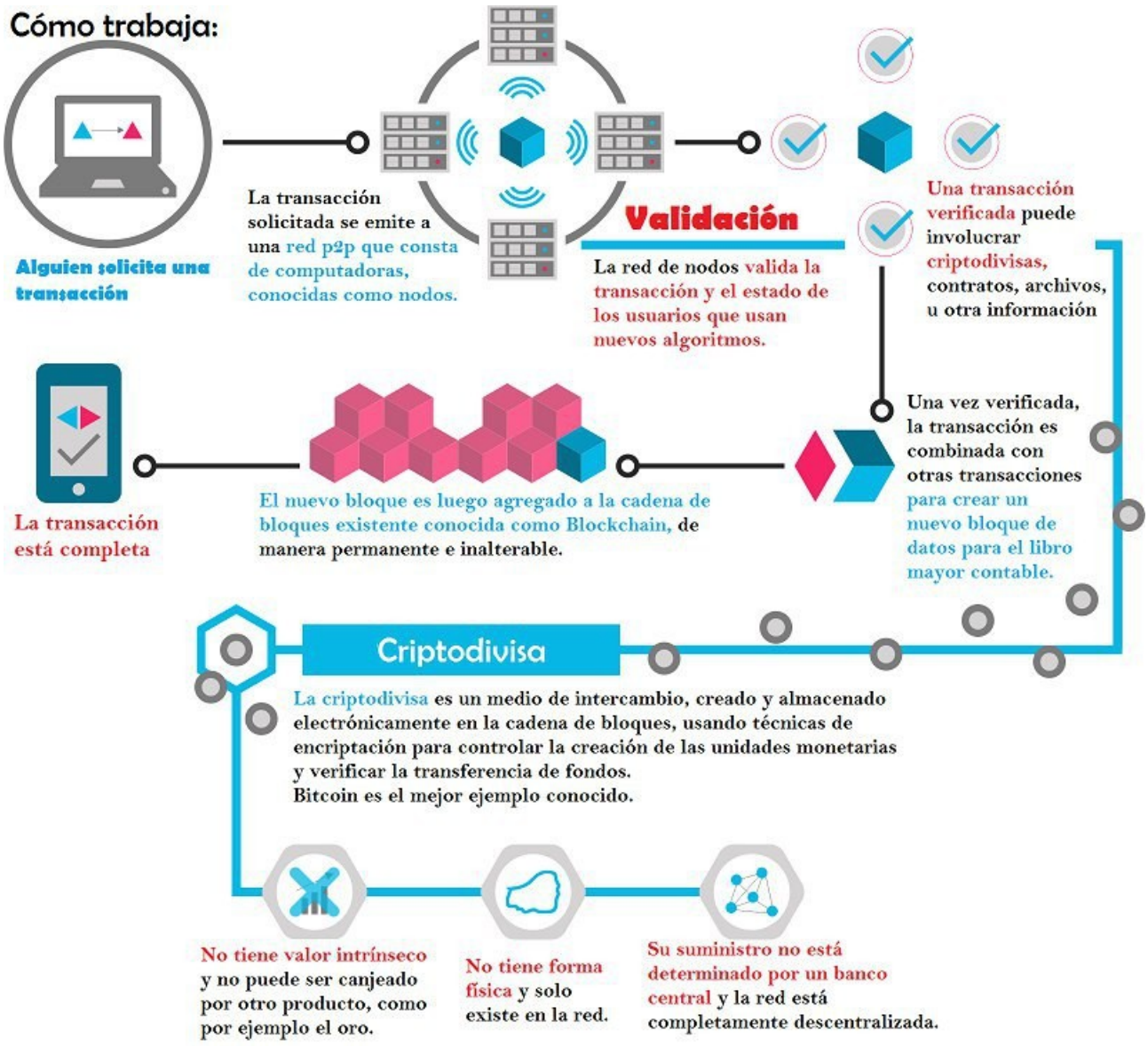
Blockchain y Transparencia

La tecnología Blockchain, tiene un valor estratégico muy alto para los procesos de transparencia institucional en todos los niveles de las Administraciones Públicas, desde la Administración General del Estado, a los gobiernos de las Comunidades Autónomas o provincias, como a nivel de los Ayuntamientos y/o Diputaciones Provinciales.

Actualmente la política está experimentando un cambio en la configuración de sus arcos parlamentarios. Cada vez son más los partidos políticos emergentes que terminan por romper los modelos bipartidistas tradicionales, sobretodos en aquellas democracias donde los escaños de los diputados se reparten a través del sistema D'hont u otros similares.

Esta nueva realidad política, plantea situaciones mucho más complejas de gobernar por la dificultad de llegar a acuerdos, o por el nivel de desconfianza entre un mayor número de partidos políticos (players).

Es precisamente aquí, donde la tecnología, y en particular Blockchain, puede aportar soluciones con niveles de seguridad y fiabilidad impensables no hace más de una década.



Ejemplos de uso de Blockchain en administraciones de Europa

-Estonia

Como caso particular en Estonia se ha establecido un programa de residencia electrónica que permite a las personas de cualquier parte del mundo solicitar su “residencia electrónica” y poder establecer un negocio. Así los “residentes” obtienen una tarjeta de identificación digital con una clave criptográfica para firmar documentos digitales, eliminando la necesidad de firmar físicamente en formularios oficiales en ventanilla.

Los ciudadanos estonios de pleno derecho pueden votar y ver qué datos tiene el gobierno sobre ellos, quién ha accedido y por qué. Hoy es uno de los pocos países donde la confianza de los ciudadanos en el gobierno ha ido en aumento.

- Dinamarca:

La primera votación con tecnología blockchain la llevó a cabo el partido político danés Liberal Alliance en la primavera de 2014, para una elección interna.

ÁMBITOS DE APLICACIÓN:

Áreas de interés estratégico con tecnología Blockchain.

El uso de blockchain en el sector público repercutirá en el voto electrónico; la contratación electrónica; la recaudación de impuestos; la emisión de pasaportes; la emisión de documentos de identidad; los registros de propiedad; los registros de sistemas de salud; y en la concesión y gestión de licencias.

- Registro Documental:

Una de las características principales de Blockchain, es el registro en libros de contabilidad descentralizados, como sistemas de notarización documental.

Dentro de los requerimientos técnicos y jurídicos de la Transparencia de la Información es precisamente la notarización de estos documentos, más allá de los sistemas de certificación y firma electrónica realizados con Certificadores Internacionales. Se ha visto que este tipo de sistemas de validación documental para certificar la autenticación de documentos oficiales están mostrando vulnerabilidades de seguridad importantes en el proceso de la transparencia de la información, como en las acciones de publicidad activa, que suponen importantes amenazas a la credibilidad y seguridad jurídica de las naciones.

Ademas creemos que puede servir como registro oficial para activos de licencias gubernamentales, propiedades intelectuales y materiales de ciudadanos y empresas, como casas, vehículos, patentes, subastas.

- GESTION ECONOMICA: Pagos y contrataciones

Confianza en la Automatización de Procesos:

La automatización de procesos dentro de la gestión pública abre un universo de proyectos que tienen como principal objetivo la desintermediación de la acción humana en procesos repetitivos, sensibles o que requieran crear un marco de trabajo de máxima confianza entre varias partes donde pueda existir desconfianza.

- Concursos públicos y licitaciones

- Contratos Públicos

- Gestión de compras

- Gestión patrimonial

Otro ámbito de aplicación está en el sector financiero, por ejemplo para detener fraudes bancarios de los comerciantes. Prevenir el fraude por medio de facturas falsas, duplicadas, usando Blockchain se crea un hash criptográfico único (una huella digital única) para cada operación.

CONTROL Y TRANSPARENCIA:

- Procesos de auditorías y redacción de informes

Por ejemplo blockchain se puede usar para "reducir el fraude, corrupción, error y el coste de los procesos que requieren mucho papel.

Facilitar a los servicios de auditoría la comprobación a través de los registros

del blockchain la ejecución de sus procedimientos.

Los procesos internos todos podrán ser auditados: periodistas, gobierno, partidos... incluso cualquier ciudadano

Un caso practico inmediato: es realizar auditoría sobre datos inmutables, datos que no pueden retocarse en fecha distinta. Poder evitar el fraude derivado, es algo diferencial.

Ejemplo de Bloque: *Dato+timestamp+responsable.*

SEGUIMIENTO DE PRESUPUESTOS

Además de permitir bases de datos públicas seguras, el blockchain también hace posible un nuevo gobierno de servicios que anteriormente no eran factibles Por ejemplo, dado que las transacciones de Bitcoin son inmutables y los registros de Blockchain de cada cuenta y transacción están abiertos a inspección pública, a informes financieros.

El sistema de compras basado en blockchain podría proporcionar garantías a los ciudadanos de que sus fondos públicos se están gastando de manera responsable.

REGISTROS:

- De documentos

- De propiedades: Catastro

- Procedimientos internos en la Administración

TRIBUTOS

Las obligaciones estatales de un ciudadano podrían cumplirse a través de un código ejecutable—un contrato inteligente—en lugar del papeleo actual. Pago de impuestos, registro de actividades económicas, etc.

Muchos de los registros de impuestos podrían ser mantenidos por organizaciones e individuos que trabajen en colaboración con el gobierno y compartiendo información. Eso quitaría la carga de gran parte de la infraestructura y las soluciones del gobierno central.

SERVICIOS:

- Atención al Ciudadano

- Transporte público:

- Gestión de flotas

- BiciMad

GOBERNANZA Y PARTICIPACION

La interacción de algoritmos de consenso, junto a los contratos inteligentes (smart contracts), propiedades para la inmutabilidad de la información en combinación con la contabilidad distribuida, hacen de la tecnología Blockchain una plataforma idónea para proyectos de gobernanza descentralizada.

La posibilidad de dar trazabilidad, anonimato, y confianza en los procesos de tomas de decisiones descentralizadas es otra de las posibilidades características de gran mayor interés para las Administraciones Públicas y el Estado.

- Votación electrónica:

Por su propia estructura y funcionamiento, blockchain puede garantizar que una persona no pueda votar más de una vez en una misma elección, al tiempo que garantiza la privacidad de su voto.

Además, al no haber ninguna autoridad central que gestione la votación no es posible manipularla, así como que cualquiera que tenga interés en ello puede auditar la elección, no sólo una vez finalizada, sino en tiempo real, a medida que se va produciendo.

El voto electrónico mejoraría la rapidez y abarataría considerablemente el coste de las elecciones y referendums, lo que permitiría hacer referendums con más frecuencia, y mejorando así la democracia. Este tipo de sistemas se podrá utilizar también para cualquier tipo devotación, por ejemplo, una consulta interna en una compañía o administracion.

Los votantes pueden acceder mediante una contraseña, a revisar la veracidad y autenticidad de la informacion. Podrás comprobar que tu voto fue el que querías, haciendo una consulta en directo a la base de datos.

ENERGIA Y MEDIO AMBIENTE

- Reciclado

- Uso de recursos que favorezcan la lucha contra la contaminación

- Redes Grid de comparticion de energía para consumidores y prosumidores.

OTRAS APLICACIONES:

DAO: Organizaciones autónomas descentralizadas

DAO son organizaciones autónomas descentralizadas que buscan establecer plataformas donde cada uno de sus miembros pueda desarrollar y ejecutar

aplicaciones que les permitan beneficiarse tanto de forma individual como colectiva.

Al ser descentralizadas y autónomas, no existe un ente que ejerza autoridad sobre la ejecución de las aplicaciones o sobre la DAO misma. Con lo cual todos los acuerdos suscritos y ejecutados por los miembros de la organización autónoma descentralizada, estarán regidos por una única “autoridad”: el código.

Sí, las DAO presentan una alternativa de gobernabilidad independiente de la influencia humana, dejándola en manos de algo mucho más simple, transparente y confiable como lo son los contratos inteligentes. No más que unas líneas de código abierto que todos los usuarios podrán revisar y decidir si están de acuerdo, o no, antes de proceder a su ejecución.

Es aquí donde florece la maravilla de las DAO: van mucho más allá de las criptomonedas y las aplicaciones financieras y elevan el debate hacia otros ámbitos, como lo es la gobernabilidad autónoma basada en los contratos inteligentes.

Las organizaciones autónomas descentralizadas colocan el poder en los miembros participantes, quienes pueden presentar propuestas a la comunidad y, luego contar con la aprobación de otros miembros, éstas se ejecutarán de forma automática siguiendo las directrices que previamente han sido aprobados por las partes involucradas y establecidos en un programa de software.

CROWDFUNDING E ICO

- Sistemas de fidelización, incentivos según políticas de bien común, recompensas por voluntariado

Los contratos inteligentes basados en Blockchain son otro uso posible de la tecnología --> Por ejemplo: una localidad emprendedora podría ofrecer un bono municipal basado en blockchain que se acumula automáticamente y pagainterés para su titular en un programa o proyecto predeterminado.

Criptomonedas locales, monedas sociales:

Permiten potenciar la economia local, y proveer opciones a personas con riesgo de exclusion social

Seguimiento de Donaciones y Ayudas: Bancos de Alimentos, ropa

Han de permitir realizar una trazabilidad tanto de ayudas oficiales como de donaciones

4.- INTRODUCCION A LOS CASOS DE USO POSIBLES EN EL AYUNTAMIENTO DE MADRID

A continuación se esbozan una serie de casos de uso en los cuales pensamos que su implementación podría tener interés para el Ayuntamiento.

Por supuesto se trata del inicio de un proceso para el cual es imprescindible realizar una serie de estudios previos de idoneidad, viabilidad, plazos de implantación, tecnologías a utilizar, procesos de comunicación, enseñanza, etc.

Votación Electrónica:

Como hemos, comentado antes la participacion y gobernanza es esencial para una administracion basada en la transparencia y una operativa de datos abiertos.

Hemos construido una pequeña Prueba de Concepto basada en Etherium, sobre los lenguajes de Solidity y Javascript

NOTA: Ver Prueba de Concepto(POC) de Votacion Electronica Etherium :

https://github.com/medialab-prado/blockchainapp/blob/master/POC_Ethereum.pdf

Linea Madrid: Cita Previa

Hemos contemplado para el ayuntamiento de Madrid, un caso practico con datos obtenidos del Dataset, correspondientes a las gestiones, de Cita Previa, del Canal de Atencion al Ciudadano LINEA MADRID.

Ver Prueba de Concepto(POC) de LINEA MADRID :

https://github.com/medialab-prado/blockchainapp/blob/master/POC-Cita_previa-Linea_Madrid.md

Transporte público:

Blockchain puede simplificar los procesos de automatizacion entre la administracion municipal y los ciudadanos, especialmente en los servicios actuales de transporte del ayuntamiento:

- EMT

- Transportes alternativos: Bicimad

Ejemplo de proyecto alternativo de Transporte basado en Blockchain:

KONECTI: www.konecti.org

En el proyecto Konecti se unen dos propuestas de valor que ya están siendo validadas en los mercados, una es la de compartir coche o “carsharing”

donde vemos que el modelo actual de poseer vehículo propio será reemplazado por un modelo de alta disponibilidad y bajo coste con un vehículo *"on demand"*.

Para eso se esta creando la primera DMO (Decentralized Mobility Organization), donde los objetivos son:

- Poblar las ciudades de coches eco-sostenibles y diseñados para el servicio con un alto nivel de disponibilidad para los usuarios
- Tokenizar y sacar al mercado no solo la propiedad de las flotas, sino la organización en sí misma.

Diseñar un sistema de incentivos individuales y comunitarios que garantice la optimización de los recursos de mobilidad y a la vez maximizar los beneficios para todo aquel que posea un token DMO.

Queremos crear no solo ciudades inteligentes, sino ciudadanos que quieran vivir y participar en ellas.

Tecnologia e Infraestructura:

La implantación de sistemas blockchain implica una serie de cambios, tanto en lo referente a los sistemas actualmente en uso, como en los procedimientos necesarios.

Para ello, lo primero que habría que plantearse es la realización de diversos estudios exhaustivos que valoren tanto la idoneidad con la viabilidad de esta implementación, así como una estimación de plazos y una estrategia de implantación.

Otro aspecto de gran importancia es la definición de la infraestructura y las tecnologías que vayan a soportar la implementación. Se debe ajustar a la legislación vigente, en lo que respecta a la privacidad de los datos que se incluyan, asi como garantizar el acceso a los usuarios afectados y establecer el seguimiento de los mismos por parte de los funcionarios y demás empleados del Ayuntamiento que necesiten acceder a los mismos.

Requirimientos minimos:

Un sistema blockchain descentralizado, puede utilizar la infraestructura de servidores actual, pues en principio se puede implementar en dichos equipos y lo único que requeriría sería la instalación de las aplicaciones necesarias para llevarlo a cabo, y un enlace de comunicaciones minimo reservado, para poder asumir las operaciones de un "full node" con el resto de la red.

Asimismo, se puede permitir a ciertas entidades, por ejemplo, diputaciones, asociaciones ciudadanas, partidos políticos, bibliotecas, centros educativos, etc. que en determinadas circunstancias y si cumplen los requisitos necesarios, se conviertan en nodos de los sistemas de blockchain y refuercen de este modo, tanto los aspectos de transparencia, seguridad de la información, acceso por parte de la ciudadanía, etc.

Integración en los sistemas de software actuales:

A través de APIs tiene una gran capacidad de integrarse con plataformas ERP, CRM, eCommerce, DB,IoT, Big & Small Data, etc.

Implementacion descentralizada: Almacenamiento distribuido de datos

La tecnología Blockchain no almacena documentos, los registros que forman los bloques son los Hash de los documentos. Es por ello que para

determinados proyectos se hace imprescindible la combinación de la tecnología Blockchain con soluciones integrales de una capa de almacenamiento distribuido de datos. Es aquí donde adquieren un protagonismo especial **IPFS y Swarm**

¿Conceptualmente cómo podemos entender lo que son?

Podríamos decir que son el equivalente a un disco duro distribuido, esto es, pensemos en un documento en PDF, imaginemos que ese documento de divide como si fuera un puzzle en cientos de miles de trozos, y que cada uno de esos trozos se guarda en la red en un equipo o nodo diferente, de tal manera que unnodo o servidor de la Red, no dispusiera información suficiente para poder interpretar ninguna parte de ese documento. Pero cuando se activará la descargar de todas esas partes, el documento se recuperaría de manera íntegra.

Esto se lleva a cabo creando una red de nodos cooperantes, cada uno de los cuales ejecuta un cliente que se ajusta a un protocolo de comunicación rigurosamente definido utilizado para almacenar y recuperar contenido arbitrario. Aprovechando el excedente de almacenamiento y ancho de banda del participante, los nodos de red proporcionan colectivamente una plataforma de hosting sin servidor.

<u>Diferencias esenciales:</u>

Swarm está específicamente diseñado para ser parte del ecosistema Ethereum. Desde el principio, siempre fue concebido como uno de los tres pilares de la próxima web, y junto a Ethereum y Whisper definen los componentes web3. Su desarrollo está guiado e inspirado por las necesidades de Ethereum (lo más importante es la necesidad de hospedar dapps, fuente / metadatos de contrato y el bloque / estado /

Mientras tanto IPFS es una solución unificadora para integrar muchos protocolos, existentes, sin estar tan vinculado a Blockchain