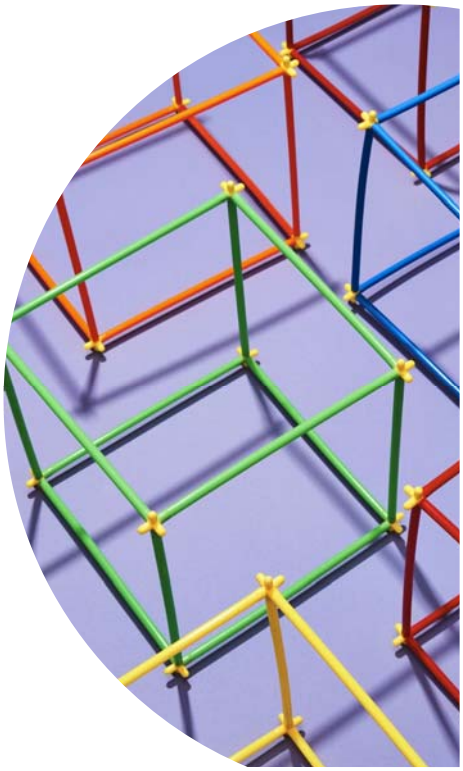
Identidad digital y soberanía de activos (autogestión)

María Jose Vañó Vañó
Directora de IUDESCOOP
Profesora Titular de Universidad
Departamento de Derecho mercantil "Manuel Broseta Pont"
Universitat de València
Miembro de BAES Lab, Universidad de Alicante
mjvanyo@uv.es

Nos introducimos en Blockchain

- *Blockchain* se ha definido por los expertos como **la tecnología más disruptiva desde la llegada de Internet**.
- B*lockchain* es una cadena de bloques cifrada y distribuida, no está centralizada, que permite hacer las transacciones de forma segura sin necesidad de intermediarios.
- Beneficios: transparencia, agilidad y eficiencia que aporta en los procesos.
- "*Blockchain* suma tecnologías que permiten crear nuevas formas de tener y distribuir valor en la red
- Su aplicación en el ámbito de las **cooperativas de viviendas** supondrá cambios tanto en los procesos de construcción, compra y alquiler, solicitud de ayudas y subvenciones, entre otros.

¿Es Blockchain la solución?



- **Blockchain no es la panacea**, ni es la única solución para dotar de seguridad a los procedimientos en la red, por ello es importante destacar algunos elementos esenciales del mismo que es fundamentalmente el **rendimiento, la estandarización o la interoperabilidad.**
  - **contribuirá a la ordenación de la información de la red.**
  - **se completa la seguridad de un procedimiento que complementará la ya ofrecida por diferentes estándares elaborados a partir de XML.**

Smart documents/Smart process

mjvanyo@uv.es

Todas las situaciones de hecho en que la información se genera, archiva o transmite en forma de comunicaciones electrónicas, independientemente de la tecnología o del medio que se haya utilizado.

Contribuye a asegurar que la ley dará cabida a las futuras novedades tecnológicas y evitar que caiga rápidamente en desuso.

La neutralidad tecnológica abarca también el concepto de "neutralidad de los medios".

mjvanyo@uv.es

IDENTIDAD Y SELF-SOVEREIGN IDENTITY (SSI)

Interconexiones

- En un **mundo interconectado** de rápido movimiento en el que las historias de vida se desarrollan en línea tanto como en el mundo real, la **confianza** se ha convertido en un mecanismo importante que es esencial en la forma en que navegamos por nuestras relaciones personales y comerciales.
- Desde **construir nuevas conexiones, perseguir intereses, hasta hacer pagos en línea, firmar acuerdos de propiedad y expandir negocios**, todo es posible en un entorno en línea siempre que haya confianza

La UE ha introducido normas para fortalecer los servicios de confianza y garantizar que nuestra actividad en línea sea segura en toda la UE

- Los servicios de confianza en sí mismos nos ayudan a autenticar estas identidades digitales:
- Firmar documentos en línea,
- recibir un recibo de venta
- asegurarnos de que estamos comprando productos reales y no falsificados.
- Evitar suplantaciones de identidad

Gracias a la tecnología, la confianza se ha transformado de algo intangible a una realidad digital.

 mjvanyo@uv.es

Actividades que necesitan de confianza:

- Confirmar nuestra identidad al acceder a cuentas en línea,
- Interactuar con AAPP
- Firmar contratos comerciales: la identificación electrónica (eID) y los servicios de confianza están habilitando nuevas tareas (firmas, reuniones en persona, sellos y cartas).
- Avanzamos en la década digital: la UE buscará generar aún más confianza en nuestras actividades diarias en línea.

 mjvanyo@uv.es

Gestión de servicios profesionales

- Aprovechar las oportunidades de negocio transfronterizas
- Aumentar la eficiencia y la seguridad de su negocio + mejorar la experiencia del usuario
- Ejemplo: En España representando a un cliente rumano en la compra de una propiedad en Francia. El cliente solicita el servicio en línea en su sitio web
  - Su empresa tiene una web calificada con certificado de autentificación que asegura que su sitio web es de confianza, lo que ayuda a evitar el phishing y aumenta la confianza del consumidor.
  - Utilizando la identificación eID del cliente, su empresa puede verificar y validar la información de los clientes electrónicamente.
  - Envío protegido de documentos para la firma de las partes garantizando su origen y su integridad.

 mjvanyo@uv.es

¿De qué se trata el Reglamento eIDAS?

El Reglamento eIDAS permite el uso de medios de identificación electrónica y servicios de confianza (es decir, firmas electrónicas, sellos electrónicos, sellado de tiempo, entrega electrónica registrada y autenticación de sitios web) por parte de ciudadanos, empresas y administraciones públicas para acceder a servicios en línea o gestionar transacciones electrónicas.

¿Qué nos ofrece eIDAs?

- transparencia y responsabilidad: obligaciones mínimas bien definidas para los proveedores de servicios de confianza (TSP) y responsabilidad;
- garantía de confiabilidad de los servicios junto con requisitos de seguridad para TSP;
- neutralidad tecnológica: evitar requisitos que solo una tecnología específica podría cumplir;
- reglas de mercado y certeza de estandarización.

¿Cuáles son los beneficios de eIDAS?

- Los ciudadanos podrán realizar transacciones electrónicas transfronterizas seguras y aprovechar plenamente sus derechos en toda la UE, desde la matrícula en una universidad extranjera hasta el acceso a la historia clínica electrónica, certificar todo el proceso de compra de una vivienda.
- Los ciudadanos que se trasladen a otro Estado miembro podrán gestionar el registro y todas las demás administraciones en línea, eliminando el papeleo.
- Las empresas se beneficiarán de menos burocracia. Las ganancias pueden ser enormes para ellos y conducir a una reducción significativa de los gastos generales.
- Las preocupaciones de seguridad y privacidad se reducen, ya que los ciudadanos y las empresas pueden usar sus propios eID nacionales para acceder a los servicios en línea.
- Los servicios ofrecidos por las AAPP se vuelven más flexibles y adecuados a las necesidades de los usuarios.

 mjvanyo@uv.es

Ventajas en los servicios profesionales

- Los servicios profesionales, incluidos, abogados, notarios, arquitectos y contadores, entre otros, pueden beneficiarse de los servicios de EID y de confianza a través de la digitalización de sus procesos de negocios. En su interacción con otras empresas y clientes, los servicios profesionales dependen en gran medida de la confianza entre las diferentes partes involucradas.
- El uso de servicios de eID y de confianza, como Leals, Esignatures y Etimestamps, simplifican para las empresas de procedimientos formales que consumen tiempo.
- eID permite que los servicios profesionales aprovechen las oportunidades de internado, como la realización de "conocer a su cliente".
- La digitalización del sector mediante el uso de los servicios de eID y de confianza reducirá la dependencia de los documentos basados en papel, al tiempo que mantiene la validez y la seguridad de los documentos que se comparten.

© Maria José Vañó Vañó mjvanyo@uv.es

Elementos clave de la eID

- **Identidad digital en la que el usuario tiene pleno control de sus datos**
- El usuario controla cada transacción de información (**qué compartir, cómo y con quien**)
- Compartir información a través de un sistema descentralizado (**blockchain/consenso**)
- Supuestos:
  - Plataformas de servicios de alquiler de viviendas o de compraventa
  - Servicios web
  - Credenciales educativas. Competencias adquiridas
  - Votación electrónica segura

Ejemplos

- eID para una verificación de confianza de la identidad de los clientes para establecer una relación contractual y cumplir con conocer los requisitos de su cliente
- *Esignature y Etimestamp* permiten a los abogados realizar acuerdos contractuales digitales sin papel que son legalmente vinculantes
- Los traductores jurados pueden usar *Real* para certificar la validez de los documentos traducidos.
- El servicio de entrega registrado electrónico le permite a cualquier profesional que envíe documentos importantes que reducen el riesgo de pérdida, robo, daño o alteraciones.

Aseguramiento de transacciones

- El desarrollo de las transacciones realizadas a través de internet obliga a asegurarlas, buscando mecanismos que consigan la **autentificación, la confidencialidad, la integridad, el no repudio y el fechado de estas**. La vía tecnológica desarrolla "taxonomías", "procolos" y "mecanismos" como el lenguaje XML (*eXtensible Markup Language*).
- XML se configura como instrumento facilitador del intercambio de información legal tanto desde la perspectiva contractual, como desde la perspectiva de intercambio de información entre organismos públicos. En el ámbito contractual permite que los contratos y su contenido sean prefijados por las partes y que sean validados con su creación, sin que se produzcan modificaciones no deseadas ni no negociadas por los contratantes. Lo que resultará sumamente útil en el comercio electrónico, al crear bases de datos estructuradas y permanentemente actualizadas, y en tiempo real.

- Aunque la *interoperabilidad* ha sido concebida en un primer momento como **un elemento puramente técnico para el desarrollo de internet**, no es menos cierto que el **legislador** ya es consciente de la necesidad de que exista una coordinación de esquemas/taxonomias y del propio lenguaje, para lo cual está delimitando los parámetros a través de normas reguladoras de la interoperabilidad.
- La elaboración de estándares que definan modelos para permitir la comparación incrementará la transparencia en el sector y los inversores encontrarán mayor seguridad en sus operaciones.
- El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea se publica a partir de la constatación de la necesidad de la instauración de una cooperación administrativa basada en la revisión del Marco Europeo de Interoperabilidad que tiene por objetivo la mejora de la colaboración digital entre AAPP en Europa.

REQUERIMIENTOS TÉCNICOS, Y VALIDEZ JURÍDICA

Principio general de IDAS

ReIDAS debe garantizar la conservación a largo plazo de la información, es decir, la validez jurídica de la firma electrónica y los sellos electrónicos durante períodos de tiempo prolongados, garantizando que se puedan validar independientemente de la evolución futura de la tecnología

Conceptos básicos: Hash

Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Propiedades deseables de una función hash según AEPD

- Permite ejecutarse sobre contenido digital de cualquier tamaño y formato. Al final, todo contenido digital son números para el ordenador: textos, fotografías, videos, etc.
- Dada una entrada cualquiera, produce una salida numérica de tamaño fijo.
- El resultado es determinista, es decir, para el mismo mensaje o conjunto de datos de entrada siempre se obtiene el mismo resultado.
- Reconstruir el mensaje original a partir del resultado de la función hash debe ser extremadamente costoso, sino imposible
- Una mínima variación en el mensaje original (un bit) ha de producir un hash totalmente distinto (difusión).
- Si se selecciona un mensaje de entrada, encontrar otro mensaje que tenga el mismo resumen ha de resultar extremadamente costoso (colisión débil).
- También ha de ser extremadamente costoso encontrar dos mensajes cualesquiera que tengan el mismo resumen (colisión fuerte).
- El algoritmo de hash deberá cubrir de forma uniforme todo el espacio de hash, los que significa que cualquier resultado de la función hash tiene, a priori, la misma probabilidad de ocurrencia que cualquier otro. Por lo tanto, todos los valores del espacio de hash pueden ser resultado de la función hash.

Descripción de una función hash

- El mensaje de entrada se divide en bloques.
- Un formula calcula el hash, un valor con un tamaño fijo, para el primer bloque.
- Se calcula el hash del siguiente bloque y suma al resultado anterior.
- Se realiza el mismo proceso sucesivamente hasta que se recorren todos los bloques.

- Las funciones hash aspiran a ser irreversibles y por ello el resultado de aplicar una función hash a un identificador directo debería de evitar la reidentificación del mismo.
- Un fichero con datos personales puede contener "identificadores" que por sí solos están asociados de forma unívoca a un sujeto (v.g. el DNI, el nombre completo o el pasaporte).
- Los ficheros con datos personales también pueden contener otros datos que, convenientemente agrupados y cruzados con otras fuentes de información, pueden llegar a identificar a un individuo. Estos datos se denominan "seudoidentificadores", "cuasi-identificadores" o identificadores indirectos22. La relación entre estos y el valor de hash se puede establecer de dos formas.
- La primera es que el hash se pueda vincular con seudoidentificadores como un efecto secundario que no es el objeto del tratamiento. El segundo caso se plantea cuando el propósito en el tratamiento es vincular seudoidentificadores entre sí mediante un valor de hash.

Identificación y servicios de confianza

Objetivo del Reglamento 910/2014:

- Nivel de seguridad adecuado a los medios de identificación electrónica y los servicios de confianza de aplicación directa a todos los estados y de manera uniforme.

En particular:

- a) las condiciones en que los Estados Miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro,
- b) las normas para los servicios de confianza, en particular para las transacciones electrónicas, y
- c) el marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

¿Qué certificados contempla el Reglamento eIDAS?

Certificado de firma: orientado a la firma de personas físicas. La firma implica la garantía de origen e integridad de los datos firmados, así como la conformidad/consentimiento con dichos datos y obligación legal respecto al contenido. Es equivalente al certificado de firma de persona física de la ley 59/2003.

Certificado de sello: orientado al sello de personas jurídicas.

- No llevan una persona custodio/responsable del certificado.
- Se orienta al sello (garantía de origen e integridad de los datos).
- Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores (Considerando 65 del Reglamento eIDAS)
- Cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica. (Considerando 58 del Reglamento eIDAS). No a la inversa.

¿Qué certificados contempla el Reglamento eIDAS? (II)

Certificado de autenticación web. Orientado a vincular el sitio web con la persona física o jurídica titular del certificado.

Certificado no cualificado. Puede estar orientado tanto a personas físicas, como jurídicas, componentes, SSL. Para persona física no se contempla su uso ya que no está recogido en la legislación vigente (Ley 39/2015), al no aportar las mismas garantías que los certificados cualificados, como por ejemplo estar sometidos a una supervisión más ligera, los requisitos de verificación de la identidad de la persona a quien se expide el certificado, o proporcionar el estado de validez o revocación de forma automatizada, fiable, gratuita y eficiente. etc.

Identificación electrónica de los interesados. Reconocimiento mutuo

Siguiendo lo dispuesto en el art. 9 de la Ley 39/2015 del procedimiento Advo. Común: nodo eIDAS

- Componente de interoperabilidad que se conecta con los servicios electrónicos y los sistemas de identificación nacionales y con los nodos de otros estados miembros. **Reconocimiento de identidades electrónicas emitidas por otros países de acuerdo con lo dispuesto en el Reglamento eIDAS**
- Obligación de reconocer los esquemas de identificación notificados por otros Estados Miembros para el acceso electrónico de los ciudadanos (personas físicas y jurídicas) a los servicios públicos

Atributos obtenidos a partir del nodo eIDAS

Los atributos que se pueden obtener a través del nodo eIDAS están definidos en las especificaciones técnicas eIDAS que están disponibles en el siguiente enlace: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile

Para personas físicas:

- Datos obligatorios
  - Identificador de unicidad (no persistente en todos los países)
  - Nombre
  - Apellido
  - Fecha de nacimiento
- Datos no obligatorios
  - Nombre al nacer
  - Apellido al nacer
  - Lugar de nacimiento
  - Dirección actual
  - Género

Atributos obtenidos a partir del nodo eIDAS

Para personas jurídicas:

- **Datos obligatorios**
  - – Identificador de unicidad
  - – Nombre legal
- **Datos no obligatorios**

– Dirección actual

– Número de registro de IVA

– Número de referencia fiscal

– El identificador relacionado con el artículo 3, apartado 1, de la Directiva 2009/101/CE del Parlamento Europeo y del Consejo (registro de sociedades)

– El identificador de entidades jurídicas (LEI)

– El número de registro e identificación de operadores económicos (número EORI)

– Número de impuestos especiales (SEED)

– Código de Clasificación Industrial Estándar (SIC)

¿En qué consiste el atributo Identificador de unicidad?

- Se trata de un identificador vinculado de manera única a una persona determinada.
- Este identificador garantiza que no habrá dos personas con el mismo identificador, pero no que la misma persona tenga siempre el mismo identificador, ya que no es completamente persistente en todos los países (una persona puede tener identificadores distintos a lo largo de su vida).
- No puede establecerse necesariamente ninguna correspondencia con el identificador real del ciudadano (por ejemplo, con su código fiscal, nombre de usuario, etc.).

Firma electrónica

La validación de certificados y firmas electrónicas se puede realizar a través de la plataforma @firma. Entre otra información, la plataforma permitirá obtener:

- País emisor del certificado.
- Nivel del certificado: avanzado o cualificado. Tipos de certificados según el eIDAS: firma (ESIG), sello (ESEAL), autenticación web (WSA) o desconocido (UNKNOWN).
- Datos básicos del poseedor del certificado.

A partir del 1 de Julio de 2016 es obligatoria la validación de todos los certificados europeos incluidos en las Listas de confianza (TSL) de sus Estados Miembros.

- para los ciudadanos españoles si está contemplada la posibilidad de identificación y firma simultanea a través de certificados.
- Para ciudadanos europeos, la identificación debería realizarse a través del nodo eIDAS con un sistema de identidad notificado y la firma mediante certificado validado por @firma.

IDENTIDAD AUTOGESTIONADA (SSI)

Identidad autosoberana/autogestionada

Elementos esenciales:

- registros descentralizados de información
- billeteras digitales

Identidad autogestionada => ¿Autosoberana?

Soberanía/autogestión para el individuo **no en la emisión de la identidad** sino en su administración y presentación a terceros

Manejo de activos y credenciales digitales (pasaporte digital, título académico, título de propiedad, divisas, euros tokenizados…)

Se elimina la necesidad de que la entidad tercera a la que se le presente un activo digital tenga que acudir directamente al emisor para comprobar su veracidad o validez (registro público y descentralizado, red blockchain)

"La identidad es la representación de una entidad en forma de uno o más atributos que permiten que la entidad o entidades se distingan suficientemente en su contexto."– UIT (ITU, 2018)

"La identidad es un conjunto de atributos relacionados con una entidad." – ISO/IEC 24760-1 (ISO, 2019): "la identificación es el proceso de reconocer una entidad en un dominio particular como distinta de otras entidades"

Derecho español: vinculada al nacimiento o a la adquisición de personalidad jurídica.

Identidad digital

- **Concepto:** conjunto finito de atributos que permite a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente.
- **Ventajas:** evitar las limitaciones del mundo físico y posibilita conexiones confiables en todo el mundo, así como transacciones y provisión y recepción de servicios digitales

Beneficios para las personas	Beneficios para el sector público	Beneficios para el sector privado
Conveniencia	Mejor prestación de servicios	Oportunidades comerciales en ciberseguridad
Utilidad	Reducción de costes de personal	Oportunidades comerciales como proveedores de identidad
Reducción de costes	Reducción de costes de procesos en papel y almacenamiento	Mayor accesibilidad de clientes
Inclusión	Reducción de costes de prestación de servicios	Facilitación de procesos de verificación de usuarios
Experiencia de usuario	Datos preparados para el análisis	Reducción de costes por prestación de servicios
	Incremento de la seguridad	

Problemas

- Regulación y estándares: ReIDAS y Reglamento General de Protección de Datos -GDPR
- Tecnología: Certificados X.509 y tarjetas chip, combinación de contraseñas e información biométrica.
  - Características que debe cumplir:
    - **Escalabilidad:** que sean adaptables y replicables.
    - **Interoperabilidad:** que permitan acceso a todo tipo de servicios públicos y privados.
    - **Portabilidad:** que permitan llevar los identificadores digitales y credenciales a cualquier lugar.
    - **Recuperación:** que permitan recuperar claves y credenciales de manera fácil y segura.
    - **Seguridad:** que protejan datos e información personal, incluidas claves privadas y credenciales.
    - **Seudónimo:** que permitan interactuar sin revelar nuestra identidad real.
  - **Utilidad:** que proporcionen valor a las personas y ofrezcan una experiencia de usuario satisfactoria.
- Seguridad:
  - No somos dueños de la información en internet sobre nosotros
  - Contraseñas
  - Vínculos entre cuentas que administran nuestras credenciales

Identidad provista por un tercero

El proveedor de identidad y el proveedor de servicios son entidades diferentes que se comunican entre sí.

Cada vez que una persona física o jurídica quiere acceder a un servicio digital ofrecido por un proveedor de servicios, deberá recurrir a su proveedor de identidad para autenticarse en su nombre.

La comunicación entre el proveedor de identidad y el servicio o recurso se realiza a través de protocolos, estándares y marcos comunes, como SAML (OASIS, 2008), OAuth (IETF, 2012) y OpenID.

Modelo federado

- existen varios proveedores de identidad que han establecido previamente acuerdos entre ellos y operan bajo un marco de confianza común.
- Este modelo puede ser tanto público y avalado por la regulación (como el eIDAS en la Unión Europea), como privado y habilitado por acuerdos privados entre las partes.
- las entidades que constituyen la federación comparten un identificador único para cada usuario. La principal diferencia entre este modelo y los centralizados y de identidad provista por un tercero es que el modelo federado es un esquema de gestión de identidad de muchos a muchos, mientras que el modelo centralizado puede verse como de uno a uno, y el tercero como uno a muchos.

IAS

Movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas. La IAS permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico".

Principios:

- **Acceso:** los usuarios deben tener acceso a sus propios datos.
- **Consentimiento:** los usuarios deben aceptar previamente el uso de su identidad por terceros.
- **Control:** los usuarios deben poder controlar sus identidades.
- **Existencia:** los usuarios deben tener una existencia independiente.
- **Interoperabilidad:** las identidades deben poder utilizarse ampliamente.
- **Minimización:** la divulgación de reclamaciones debe reducirse.
- **Persistencia:** las identidades deben ser duraderas.
- **Protección:** los derechos de los usuarios deben ser protegidos.
- **Portabilidad:** la información y los servicios sobre identidad deben ser portables.
- **Transparencia:** los sistemas y algoritmos deben ser transparentes.

Desafíos de la SSI

Adaptación la infraestructura y modelos de datos digitales:	Análisis y comprensión de la tecnología por juristas, notarios y reguladores	Billeteras digitales	Captación de usuarios	Copias de seguridad
Derecho al olvido	Marcos de confianza	Participación de los gobiernos	Políticas regulatorias	Privacidad
Protección de datos	Pruebas de conocimiento cero	Reconocimiento de estándares	Recuperación de claves	Registros descentralizados madureos
	Seudónimo	Uso de la biometría		

Ventajas para las cooperativas de viviendas

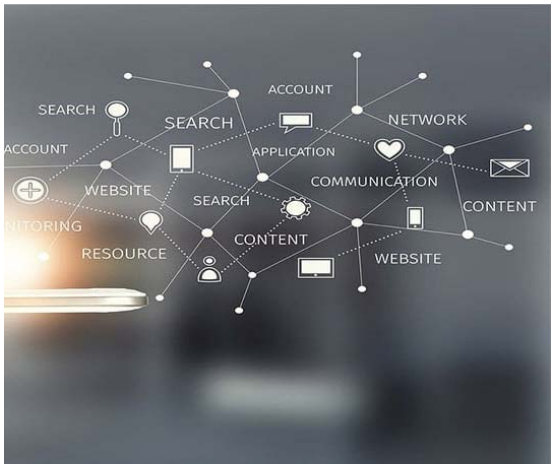
- Certificación de los documentos e hitos en el proceso de promoción. Seguimiento del procedimiento. Garantía de confianza al cliente y al posible inversor y a la entidad promotora.
- Validación de documentos por parte de los técnicos responsables y certificación de los datos en la cadena de bloques blockchain.
- Barrera: Falta de confianza y desconocimiento

Hablemos de Smart contracts

- Tecnología blockchain que permite que los datos a transmitir sean trazables, descentralizados e inalterables. No existe una única copia sino que todos los nodos comparten información a la vez.
- Smart contracts: Se ejecutan de forma automática al cumplir las condiciones prefijadas.
- Conexión de compradores, vendedores, arrendatarios, arrendadores, cooperativistas… a través de plataformas p2p sin intermediarios.
  - Tokeinización (Carmen Pastor mañana): para adquirir viviendas o partes de las viviendas, en alquiler o compra y mantenimiento de los edificios.
  - Identidad digital: Mejora la experiencia de cliente y digitalizan el proceso de adquisición de la vivienda.

© Maria José Vañó Vañó mjvanyo@uv.es

Blockchain cambia la forma en que accedemos a la vivienda (PROPTECH)



- Instant Property Network (IPN): Creada por el consorcio r3, es una plataforma para gestionar las transacciones entre los distintos actores del sector inmobiliario mediante tecnologías DLT.
- Propy: Fundada en Palo Alto (Estados Unidos) en 2015. Primera venta de un inmueble con 'blockchain' en 2017. Permite al comprador ponerse en contacto con el vendedor y conocer su registro e información de la propiedad así como el pago con 'bitcoins'.
- Shelterzoom: Es una plataforma basada en 'blockchain' para transacciones de bienes inmuebles que se puede integrar con cualquier sitio web de bienes raíces. Construido sobre la plataforma Ethereum, ShelterZoom incluye una aplicación móvil que los compradores pueden usar para enviar sus ofertas y recibir notificaciones durante el proceso de compra.
- Bitrent: Fundada en Londres en 2016, BitRent es la primera plataforma inmobiliaria de 'blockchain' que **conecta a los promotores inmobiliarios con inversores de todo el mundo** y atrae inversiones en las primeras etapas de la construcción del inmueble. Se invierten pequeñas cantidades y se protegen al registrarlas en el registro descentralizado.
- Blocksquare: Fundada en 2017 en Liubliana (Eslovenia) la plataforma permite a las compañías inmobiliarias crear y ofrecer ofertas de inversión con 'tokens' y permite vender un activo inmobiliario a hasta 100 compradores.

© Maria José Vañó Vañó mjvanyo@uv.es

Usemos blockchain

- Las transacciones en el sector inmobiliario requieren una atención especial de las AAPP en la medida en que les corresponde la carga de supervisar y dotar de seguridad jurídica a las transmisiones de propiedad.
- Venta
  - Control fiscal, legal, registral, administrativo
- Construcción
  - Información de cada una de las fases de la construcción, financiación, sujetos
- IoT y Blockchain: trazabilidad completa
  - …

 mjvanyo@uv.es

Configuremos un modelo de identidad digital

- Que permita que personas, organizaciones y usuarias de la red desarrollen relaciones con plenos efectos legales
- Que se establezcan los límites legales y las barreras correspondientes sobre la identidad de las personas físicas (GPDR) para compartir sus datos con otro agende de la cadena (notario) para lo que se requiere un modelo de identidad digital, fuerte.
  - Capacidad jurídica y capacidad de obrar => Verificación ¿notarial?
  - Titularidad del inmueble objeto de negocios jurídicos => Privado, Bien demanial
  - Negocio jurídico:
    =>Cesión en uso del suelo
    =>Compra venta
    =>Arrendamiento
    =>Masovería urbana

 mjvanyo@uv.es

Gràcies

Gracias

María Jose Vañó Vañó
Directora de IUDESCOOP
Profesora Titular de Universidad
Departamento de Derecho mercantil "Manuel Broseta Pont"
Universitat de València
Miembro de BAES Lab, Universidad de Alicante
mjvanyo@uv.es