

Credentials in **blockchain**

# CowStamp

my certificate, my proof





# CowStamp

La plataforma que permite gestionar  
**credenciales digitales verificables**  
siguiendo los estándares más avanzados  
con registro en la **blockchain**.

*my certificate, my proof*



# Credenciales digitales, vamos a situarnos

Para entender y explicar qué es una credencial digital antes tenemos que definir algunos **conceptos claves**.



# ¿Qué es una credencial digital **verificable**?

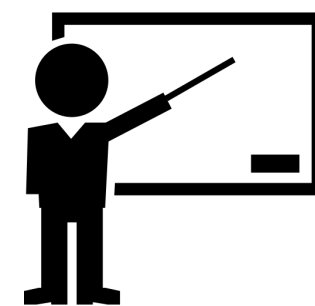
Credencial digital verificable



## Credencial digital verificable

Es una **documento digital** con una estructura definida a la que llamamos **insignia**, que permite a un **emisor** **certificar una información** y dirigirla a un **receptor**.

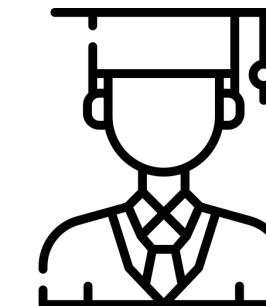
Las credenciales digitales registradas en la blockchain **permiten demostrar** a un receptor la adquisición de una o varias competencias, o de una o varias características **de forma certificada**.



**Emisor**



**Credencial**



**Receptor**



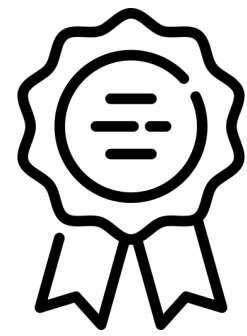
# Primero unos **conceptos** básicos

Conceptos básicos



## Certificado

Fichero emitido por una **entidad de confianza**, que permite la firma y/o cifrado de archivos.



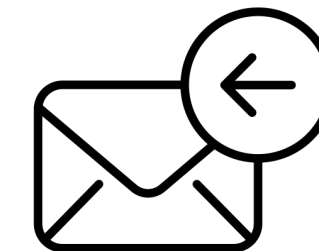
## Insignia

Estructura de datos que contiene una **información, hecho o logro** que se acredita.



## Emisor

**Quien genera el mensaje** en forma de credencial y lo envía hasta un receptor.



## Receptor

También llamado sujeto, es la persona o entidad que **recibe la credencial**.



# El origen de las Credenciales

**Mozilla Foundation y IMS Global** proponen un protocolo de emisión de credenciales digitales creando un estándar internacional *open-source* llamado **Open Badges**, a finales de los años 90.

La aparición de la tecnología **blockchain** lo cambia todo. Sus propiedades intrínsecas proporcionan nuevas herramientas que obligan a los anteriores estándares a adaptarse para poder hacer un paso adelante y poder ofrecer nuevas aplicaciones.



# Con la *blockchain* todo cambia

Credenciales a la *blockchain*



La disrupción de la tecnología *blockchain* obliga a adaptar los estándares actuales para su inclusión, es por ello que el *MIT Media Lab* define una implementación del estándar de **Open Badges**, denominada **Blockcerts**, que permite el registro de las **credenciales digitales** en la *blockchain* con la información necesaria para ser validados y aceptados.

El uso del protocolo de **Blockcerts** introduce la necesidad de realizar transacciones a una blockchain para registrar pruebas de los documentos digitalizados y, por ende, aprovechar las propiedades de la *blockchain*: **firma digital**, **timestamp**, **distribución de la información e inmutabilidad de los datos**.





Sin embargo, el estándar de Blockcerts en su versión 2.1 **no define la gestión de la identidad del emisor**, por lo que se trata de un sistema incompleto que no permite validar la identidad real de quién emite el documento registrado a la *blockchain*. De esta forma dichas credenciales no pueden tener carácter legal al poder ser **suplantada la identidad del emisor**.

Para romper con esta limitación, BTC Assessors extiende un nuevo estándar denominado **Cowcerts** el cual, permitiendo la **gestión de la identidad del emisor**, incrementa la usabilidad de las credenciales digitales pudiendo otorgar validez legal a las mismas.

La plataforma de uso **CowStamp** esta basada en el estándar de **Cowcerts** y, por ello, es totalmente compatible con todos los estándares anteriores.





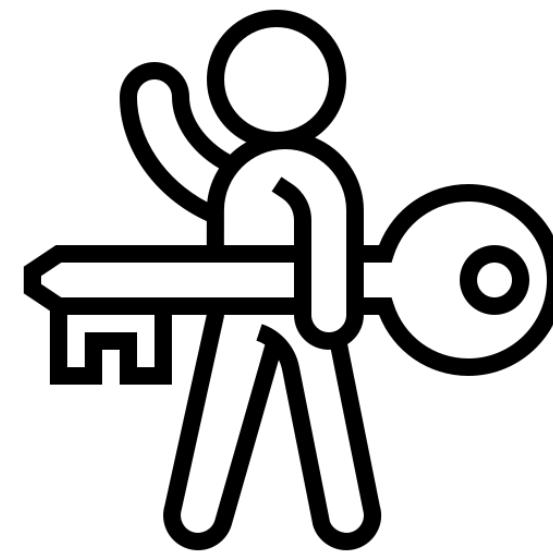
# Blockchain la revolución de la certificación

La tecnología **blockchain** en el ámbito de la certificación ha revolucionado el sector con las **credenciales digitales verificables**, permitiendo validar la integridad de las mismas y el momento en el que ha sido registrada.



# ¿Qué aporta la certificación en **blockchain**?

Introducción



## Firma Digital

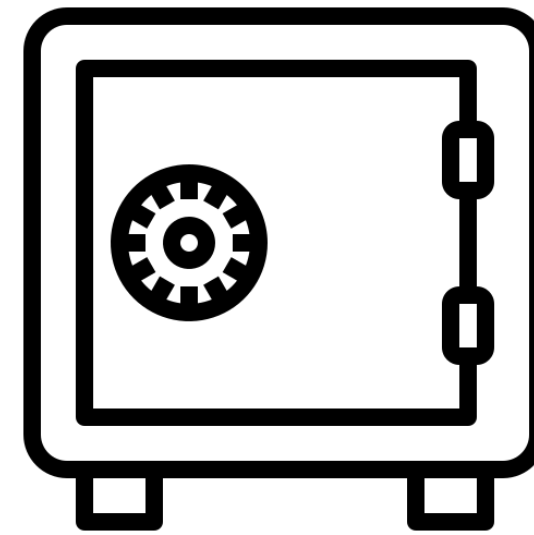
La **firma digital** es un aspecto clave en la certificación de credenciales en la **blockchain**.

Cada vez que registramos una prueba en la blockchain debemos realizar una firma digital. Por ello cada prueba registrada va asociada a la **firma digital del emisor**.



# ¿Qué aporta la certificación en **blockchain**?

Introducción



## Inmutabilidad

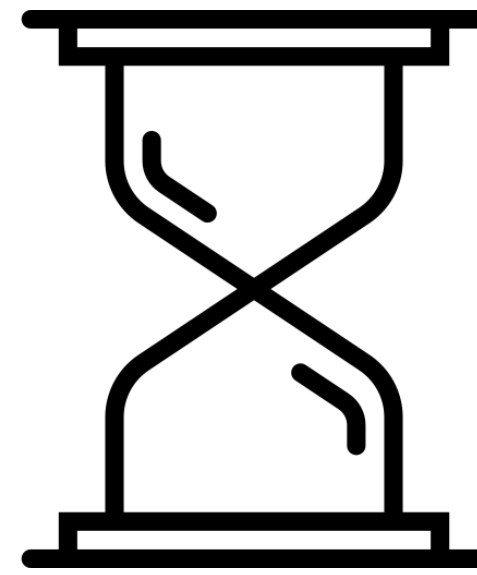
Una de las características más importantes de una **blockchain** con un buen diseño es la **inmutabilidad de los registros** incluidos en los bloques.

El hecho de poder registrar una prueba de la credencial digital en la **blockchain** nos garantizan que la prueba registrada no ha podido ser manipulada.



# ¿Que aporta la certificación en **blockchain**?

Introducción



## Timestamp

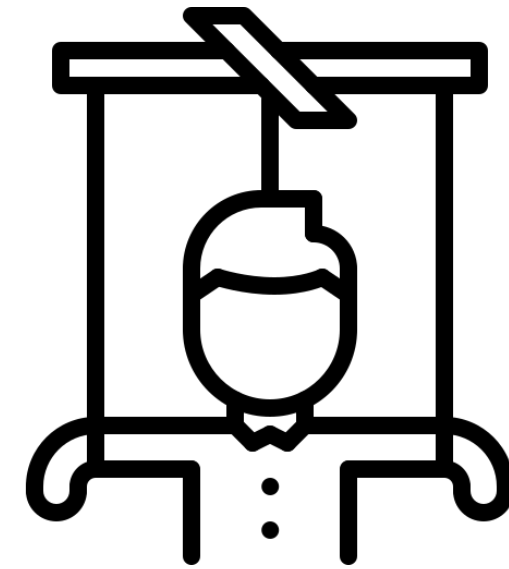
Una de las características principales de la **blockchain** es la **marca de tiempo** que se incluye en cada bloque.

La marca de tiempo o **timestamp** permite validar en qué momento fue registrada un credencial digital, **evitando posibles fraudes** o falsificaciones en la fecha de emisión.



# ¿Qué aporta la certificación en *blockchain*?

Introducción



## Sovereignty

La tecnología *blockchain* nos permite construir un ecosistema donde cada usuario es **soberano de su información**. Haciendo posible compartir solo la **información de interés**, en un formato que pueda ser validado sin mostrar más datos de los necesarios.

De esta forma, las credenciales contienen solo la información necesaria para ser validadas, protegiendo la identidad del usuario y evitando el control abusivo que puedan realizar **terceras entidades** sobre sus datos.



Las credenciales digitales verificables son el futuro de la certificación, ¡y el futuro sucede ahora!

¿Cómo puedo gestionar mis credenciales verificables?

CowStamp



Building  
the future  
Block by Block



# ¿Qué es CowStamp?

## CowStamp

Es la plataforma de gestión de credenciales digitales que permite crear, emitir y recibir **credenciales verificables** registradas en la **blockchain**, siendo compatible con **Blockcerts** y siguiendo el estándar de **Cowcerts**.



Building  
the future  
Block by Block



# ¿Que ofrece CowStamp?

Características



## Validación de la Identidad Digital

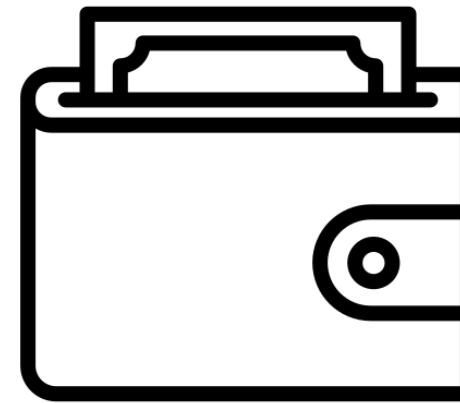
Posibilita **validar la identidad del emisor** de las credenciales mediante las redes sociales y/o el certificado digital emitido por un estado o entidad acreditada (X509).





# ¿Que ofrece CowStamp?

Características



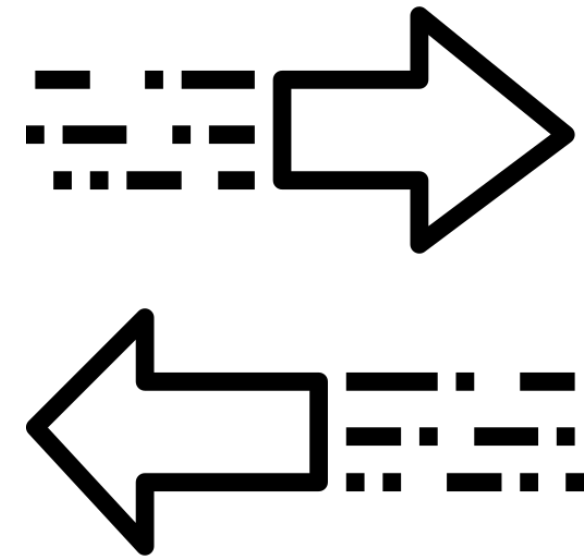
## Opción de utilizar múltiples *wallets*

**CowStamp** se integra con los **wallets** más populares, permitiendo gestionar las llaves criptográficas de la forma más segura posible sin olvidar la usabilidad de la plataforma; permitiendo así registrar en **múltiples blockchains** des del **wallet de elección**.



# ¿Que ofrece CowStamp?

Características



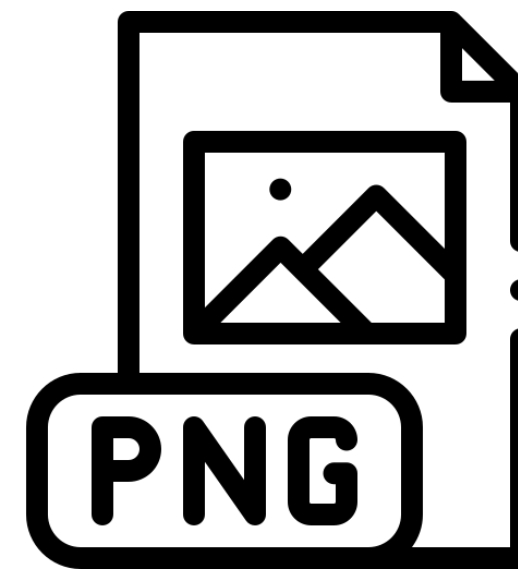
## Emisión y recepción de credenciales

La facilidad para **emitir y recibir credenciales** se realiza mediante un entorno *userfriendly* que permite la **visualización**, la **gestión** y la **validación** de las credenciales verificables de la forma más fácil y rápida posible.



# ¿Que ofrece CowStamp?

Características



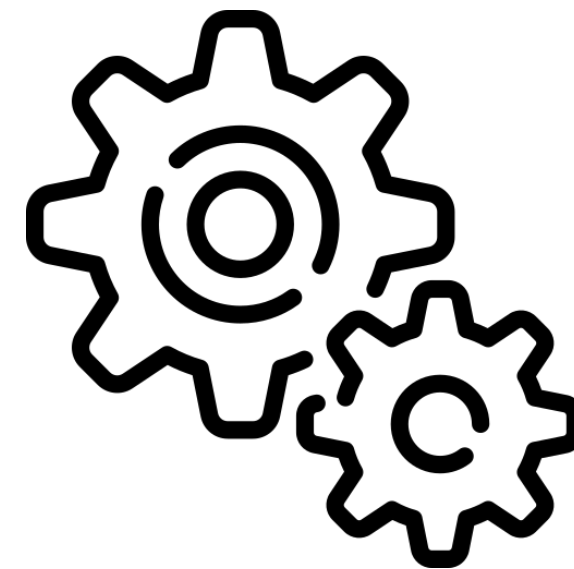
## Credenciales en formatos comprensible

La emisión de credenciales digitales con registro en la blockchain, con **CowStamp**, se efectúa bajo un **formato fácilmente interpretable** para todos los dispositivos gracias al uso de archivos de formato abierto **PNG**.



# ¿Qué ofrece CowStamp?

Características



## Aceptación de diferentes esquemas

La implementación de **múltiples esquemas de insignias** en el estándar **Cowcerts** permite la creación y validación de credenciales más complejas, siendo esto una novedad en el sector.

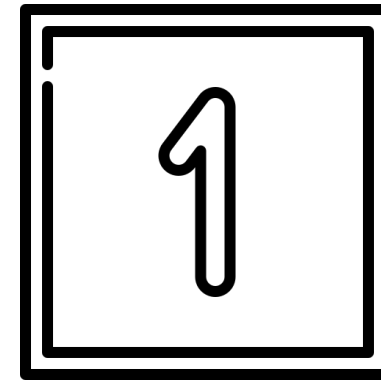


# ¿Cómo emitir una credencial con CowStamp?

La emisión de una credencial digital verificable con **CowStamp** está **simplificada al máximo** para que sólo con el registro del usuario en la plataforma, y siguiendo 5 sencillos pasos, se puedan emitir las credenciales.

# ¿Quién **emite**?

Credenciales en 5 pasos



## Crear un emisor de la credencial

Lo primero que necesitamos es **definir quién va emitir** las credenciales, ya sea una institución o un particular, por ello en **CowStamp** se crea un **emisor de credenciales**.



# ¿El emisor es **válido**?

Credenciales en 5 pasos



## Validar la identidad del emisor

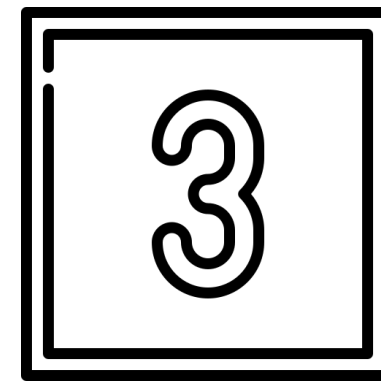
Para poder otorgar validez legal a la credencial, es imprescindible generar **pruebas de la identidad** del emisor.

Por ello, **CowStamp** permite relacionar la identidad digital del emisor en la *blockchain* con sus perfiles en las **redes sociales**, **DID** o los posibles **certificados digitales** expedidos por instituciones de confianza.



# ¿Qué **información** se certifica?

Credenciales en 5 pasos



## Definir la información de la insignia

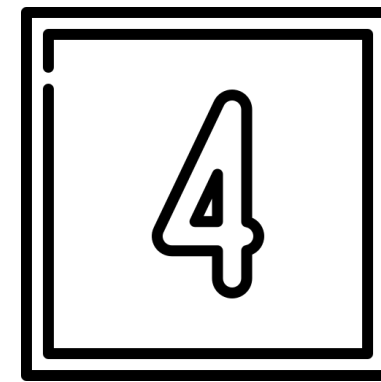
El proceso de creación de una credencial requiere **especificar el contenido de la insignia** que queremos emitir, por ello debemos definir el logro o acción que representa la credencial que vamos a otorgar a un sujeto en cuestión.





# ¿Quién es el receptor?

Credenciales en 5 pasos



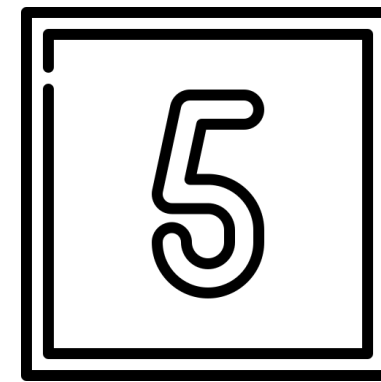
## Asignar un receptor de la credencial

Para poder emitir una credencial necesitamos **otorgar una insignia a un sujeto o receptor**. Para ello, el emisor deberá introducir los datos personales del sujeto receptor de la insignia en la plataforma.



# Registramos la prueba

Credenciales en 5 pasos



## Registrar en la blockchain el certificado

Realizar el registro del certificado en la *blockchain* es el acto que va a dotar al certificado de una **firma digital**, registrando una **prueba inmutable** del documento con **marca de tiempo** para su posterior validación.



# Ya tengo mi **credencial verificable**, ¿y ahora qué?

Cuando una entidad o persona nos emite una **credencial verificable** en **CowStamp**, des de la plataforma obtenemos un **archivo digital** en formato .JSON o .PNG que se puede validar y compartir de forma sencilla.



Building  
the future  
Block by Block

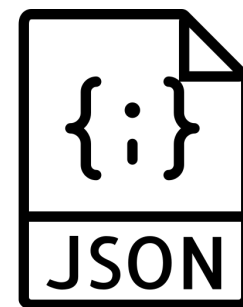




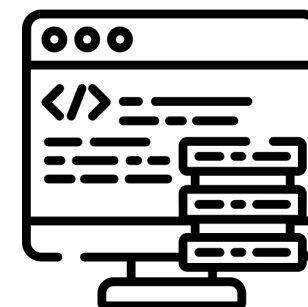
## Visualizar mi credencial

**CowStamp** crea sus credenciales digitales en formato PNG, haciendo que cualquiera pueda **visualizar la credencial** de forma sencilla.

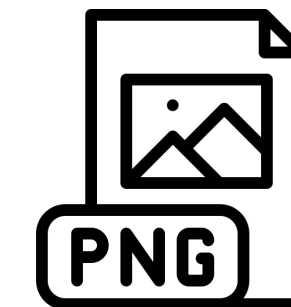
La relación entre la información que visualizamos y el contenido de la credencial es fundamental para evitar falsificaciones. Por ello, es **CowCerts** que define un estándar de visualización determinista que puede ser comprobado en el momento de la validación.



Información **contenida** en la credencial verificables



Crea un formato de visualización **determinista** a partir de la información



Formato de **visualización fiable** de la credencial

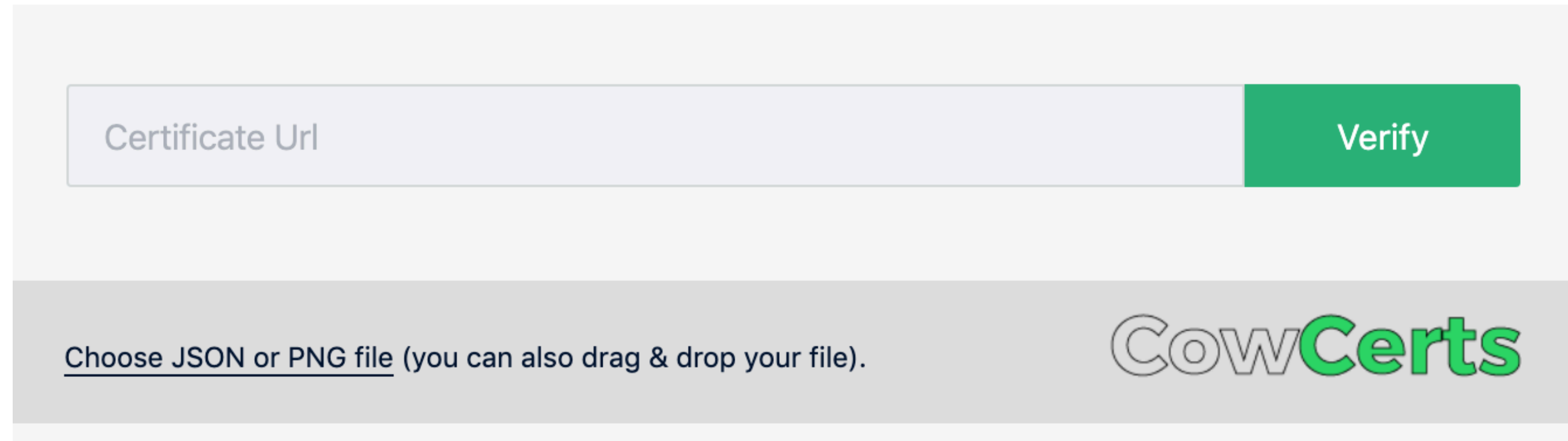




## Validar mi credencial

Para aprovechar las propiedades de las credenciales digitales es básico poderlas compartir con terceros y que éstos, de **forma independiente**, puedan **validar la información** contenida de forma segura.

**CowStamp** proporciona un validador de credenciales digitales compatible con **Blockcerts** que incluye también la validación de la **identidad** y la validación de la **visualización** siguiendo el estándar de **Cowcerts**.

A screenshot of the CowStamp validation interface. It features a light gray background. At the top, there is a white input field with the placeholder text "Certificate Url" and a green "Verify" button to its right. Below this, there is a gray bar containing the text "Choose JSON or PNG file (you can also drag & drop your file)." on the left and the "CowCerts" logo on the right. The logo consists of the word "Cow" in a light gray sans-serif font and "Certs" in a bold green sans-serif font.

Certificate Url

Verify

Choose JSON or PNG file (you can also drag & drop your file).

CowCerts



# ¿Qué casos de uso tienen las credenciales de CowStamp?

La implementación de diferentes esquemas y la rápida adaptación a los nuevos estándares de emisión y validación, hacen que CowStamp pueda adaptarse a diversos sectores y aplicarse en **múltiples casos de uso**.





## Educación

El Gobierno de Malta, y posteriormente el *Govern d'Andorra*, han sido los primeros países en implementar mecanismos de emisión de títulos académicos con registro en la blockchain, siendo el gobierno de Andorra el primero en aplicar un estándar que válida la identidad del emisor (Cowcerts).

La aplicación de la emisión de títulos en formato digital siguiendo el estándar de Cowcerts ha permitido al sistema educativo:

- Agilizar la comunicación entre el ministerio y universidades.
- Disminuir los costes de emisión de los títulos y el suplemento europeo.
- Facilitar el acceso a las credenciales digitales por parte de los estudiantes.
- Automatizar la validación de documentos y firmas digitales.







## Educación

Actualmente, y debido a los costes y complejidad del proceso la certificación académica en formato analógico, no se reconocen los conocimientos adquiridos hasta completar un conjunto determinado de estos agrupándolos bajo el nombre de una titulación académica.

La aplicación de credenciales digitales permite modificar este paradigma, creando credenciales de conocimiento a medida que se van adquiriendo. De este modo sería factible:

- Demostrar los conocimientos obtenidos antes de finalizar una titulación académica.
- La convalidación de asignaturas automáticamente.
- La concesión de becas meritocráticas de forma automática.







## **Sanidad**

Las credenciales digitales pueden tener un peso importante a la hora de construir una historia clínica soberana, creando credenciales por parte de los profesionales sanitarios que validen los actos médicos realizados, permitiendo así al usuario ser propietario de su historial médico y pudiendo compartir su información sin depender de una institución.

Un ejemplo de aplicación en el entorno sanitario y historial clínico sería la transformación del carnet de vacunas. Actualmente, en la mayoría de países el carnet de vacunas es en formato analógico, la digitalización de este se podría realizar utilizando credenciales digitales. De este modo el receptor de la vacuna obtiene un credencial con la información de la vacuna inoculada, el profesional que ha realizado el acto y del momento en que se ha realizado sin posibilidad de ser manipulado a posteriori.





## Sanidad

- Agiliza en la emisión y gestión de credenciales verificables  
Las credenciales que emite al instante el profesional cualificado, son gestionadas de forma digital evitando pérdidas o robatorios y facilitando la posibilidad de compartir la credencial en caso de ser necesario.
- Optimización de recursos  
La transformación del formato de soporte de la credencial (analógico/digital) minimiza los recursos necesarios para emisión, conservación y validación del documento.
- Permite verificar las credenciales de forma descentralizada  
Las credenciales soberanas nos permiten validar el contenido de las credenciales en cualquier parte del mundo sin depender de un servidor central, permitiendo limitar el tiempo que se comparte una credencial.
- Imposibilidad de manipular los datos  
Al registrar a la blockchain las credenciales es imposible manipular el contenido y la marca de tiempo. Por ello se puede demostrar en momento en que se registro el certificado, sin la posibilidad de indicar que un evento se efectuó en otro.





## **Automoción**

La gestión de los documentos asociados al vehículo como son la cartilla de circulación, el seguro del vehículo o la verificación de la inspección técnica, son los documentos asociados al vehículo que acreditan que podemos circular. La gestión de esta documentación no siempre es lo ágil que el usuario desea y al ser en formato analógico la probabilidad de no llevar toda la documentación en el vehículo es alta.

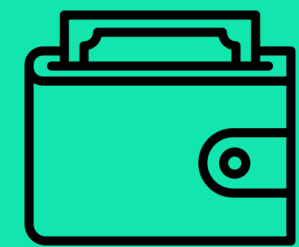
Aplicar el sistema de credenciales verificadas en blockchain en el sector de la automoción, permitirá la validación de la documentación asociada a un vehículo sin la necesidad de tener que llevar dicha documentación en el interior del vehículo. Al mismo tiempo el se podría incrementar la seguridad en las vías de circulación al poder comprobar de forma automática mediante cámaras de tráfico, si un vehículo tiene toda la documentación para poder circular.



# RoadMap de CowStamp



Soporte a IPFS



Servicio de  
Wallet  
integrado



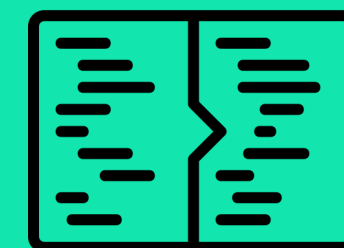
JSON  
contenido en  
PNG



Badges store



Uso de Identidades  
descentralizadas DID



Credenciales  
combinadas



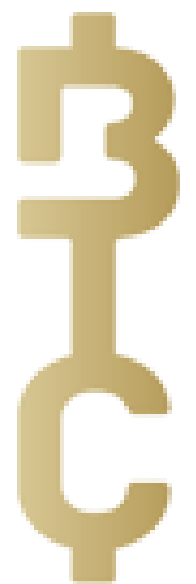
Building  
the future  
Block by Block



# CowStamp



CowStamp.com



Building  
the future  
Block by Block