



Agencia de Tecnología
y Certificación Electrónica



ACCV

Retos de la administración ante el Blockchain

Que es la ACCV?

- Agencia de Tecnología y Certificación Electrónica
 - Prestador de Servicios de Confianza Cualificado
 - eIDAS (Normativa Europea)
 - WebTrust/WebTrustBR
 - ISO 27001
 - Iniciativa pública
 - Proyecto iniciado en Generalitat Valenciana en 1999
 - Operativa desde 2001
 - Ente prestador independiente en 2007
 - Mas de 2 millones de certificados emitidos
 - Mas de 100 millones de sellos de tiempo anuales

Que es la ACCV?

- Tercera parte de confianza
 - Garantiza
 - Identidad
 - Certificados de Ciudadano
 - Pertenencia a organización
 - Certificados de empleado público
 - Tiempo
 - Sellos de tiempo
 - Representación
 - Certificados de representante
 - Registro de Representantes

Que es la ACCV?

- Servicios de confianza adicionales
 - Certificación de publicaciones
 - Certifica el inicio de difusión de una publicación
 - Códigos seguros de verificación
 - Firma centralizada
- Otros servicios
 - Soporte a usuarios
 - APIs de desarrollo (Arangí)
- Información en:
 - <https://www.accv.es>

Blockchain - Sector Público

- Ventajas inherentes a la tecnología Blockchain
 - Transparencia
 - Integridad
 - Anonimato
 - Trazabilidad
- Proyectos
 - Administración electrónica
 - Participación ciudadana
 - Auditoria pública

Blockchain - ACCV

- Necesidad de identificación fuerte
- Smart Contracts ↔ Tramite electrónico
- Filosofía híbrida
 - Descentralizada
 - Acceso ciudadano
 - Smart contracts
 - Centralizada
 - Información de búsquedas
 - Almacenamiento de información sensible

Blockchain - ACCV

- Puntos en comun
 - Tecnología de clave publica
 - Criptografía en la base de toda la infraestructura
- Diferencias
 - Tercera parte de confianza frente a confianza distribuida
 - Identidad fuerte frente a pseudo anonimato
- Necesidad de establecer relaciones entre claves
 - Par de claves ECDSA secp256k1
 - La identidad en BC se basa en solamente en la posesión de la clave privada

Blockchain - ACCV

- ACCV puede firmar la parte pública y vincularla a una identidad fuerte
 - Procedimientos bien establecidos y normalizados para asegurar la identidad
 - Una red de Puntos de Registro de gran capilaridad en la CV.
 - Permite utilizar el mismo par de claves para operar con la administración y realizar firma digital cualificada (según verificación de la identidad)
 - No interfiere con el funcionamiento normal de BC

Blockchain - ACCV

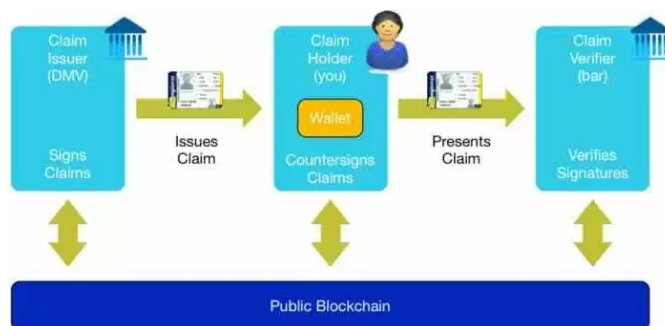
- Posibles casos de uso
 - Voto electrónico
 - Identificación fuerte para validar al votante
 - Anónima para el voto
 - D-Cent, TIVI
 - Smart contracts asociados a tramites
 - Firma digital con identidad fuerte para el SC
 - BC guarda y registra la transacción asociada a la dirección anónima
 - DAPPS como sustituto de las Plataformas de Administración Electrónica tradicionales

Blockchain - ACCV

- Posibles casos de uso
 - Licitación administrativa
 - BC garantiza transparencia, integridad y trazabilidad
 - Prevención del fraude
 - Identificación fuerte ↔ ACCV
 - Gobierno de Aragón, EJIE SA
 - Portales de transparencia
 - Información publica no modificable
 - Identificación fuerte y firma cualificada de los gestores
 - Acceso anónimo a los documentos

Blockchain - ACCV

- Posibles casos de uso
 - self-sovereign identity (identidad digital auto-soberana)
 - Necesidad de vincular las claves BC a la identidad real
 - Toda la información esta en posesión del usuario
 - ACCV como garante TTP (ente emisor)
 - Transforma las pruebas del usuario en testimonios (Phillip Windley)



Blockchain - ACCV

- Posibles casos de uso
 - self-sovereign identity (identidad digital auto-soberana)
 - CEN Workshop 84 on a 'Self-Sovereign Identifier(s) for Personal Data Ownership and Usage Control' (**CEN WS ISAEN**)
 - Individual perSonal data Auditable addrEss Number.
 - Conforme a la EU GDPR/eIDAS
 - Inicialmente solo para personas físicas
 - Sovrin, Selfkey
 - PKI actúa como un actor proporcionando las características
 - Acceso
 - Control
 - Portabilidad
 - BC se utiliza para almacenar DID (Identificadores descentralizados)

Blockchain - ACCV

- Posibles casos de uso
 - Identidad económica
 - Proyectos solidarios
 - Permiten realizar transacciones sin acceso a cuentas oficiales
 - Acceso para refugiados y personas invisibles económicamente
 - Banq
 - No hace falta cuenta bancaria
 - Se necesita teléfono móvil o equivalente
 - Sistemas de contacto entre refugiados/desplazados
 - Bitnation Refugee Emergency Response (BRER)
 - Fundación IOTA /Refunite
 - Ayuda gubernamental a la Inmigración
 - Gobierno de Suiza, Gobierno de Finlandia, Gobierno de EEUU

Blockchain - ACCV

- Problemática
 - Burbuja tecnológica
 - Tecnología con gran posibilidad de crecimiento y muchas aplicaciones
 - Peligro de expectativas inalcanzables
 - Incremento de la brecha digital
 - Difícil de entender para el usuario
 - Peligro de dejar fuera a sectores menos formados