www.uib.cat

RECSI 2022

E-TICKETING MEDIANTE NFTs

Maria Magdalena Payeras-Capellà
Macià Mut-Puigsever
Jordi Castellà-Roca
Jaume Ramis-Bibiloni
Llorenç Huguet-Rotger
Miquel À. Cabot-Nadal

UIB Universitat de les Illes Balears #SOM UIB

Santander 19-21 Octubre 2022
XVII Reunión Española sobre Criptología y Seguridad de la Información

ÍNDICE

Introducción

INTRODUCCIÓN

Ticket:

la representación del derecho de su propietario a usar un determinado servicio.

INTRODUCCIÓN

NFT (Non Fungible Token):

- Representan la existencia y la propiedad de diferentes activos (vídeos, imágenes, obras de arte, tickets, …).
- Se basan en un contrato inteligente en una red blockchain.

RECSI 2022

INTRODUCCIÓN

CHAMPIONS

La UEFA desmonta las cifras del gobierno f… sobre el caos … Cham…

Binance incursiona en la venta de entradas NFT tras el fiasco de la Liga de la UEFA

Binance colaboró con la Società Sportiva Lazio para lanzar entradas NFT para todos los partidos en casa del club deportivo en el Stadio Olimpico.

INTRODUCCIÓN

OBJETIVO:

- Analizar si el uso de NFTs puede satisfacer los requisitios de los sistemas de e-ticketing …
- ... evaluando sus retos y oportunidades.

Tokens no fungibles

TOKENS FUNGIBLES VS. NO FUNGIBLES

ESTÁNDARES ERC - BLOCKCHAIN ETHEREUM

ERC-20: estándar para tokens **fungibles.**

Intercambiables entre sí, ya que todos son iguales.

ERC-721: estándar para tokens **no fungibles.**

Cada token es un activo único distinguible y tiene un propietario.

FUNGIBLE	NON-FUNGIBLE
Dollar	Digital Art
Bitcoin	Physical Art
Gold	Property

Cada NFT tiene un tokenID que es globalmente único.

TOKENS NO FUNGIBLES

USOS ...

- Artículos multimedia
- Acciones
- Puntos en sistemas de fidelización
- Incentivos
- Certificación de propiedad de activos
- Premios
- Títulos
- ...

RECSI 2022

e-ticketing

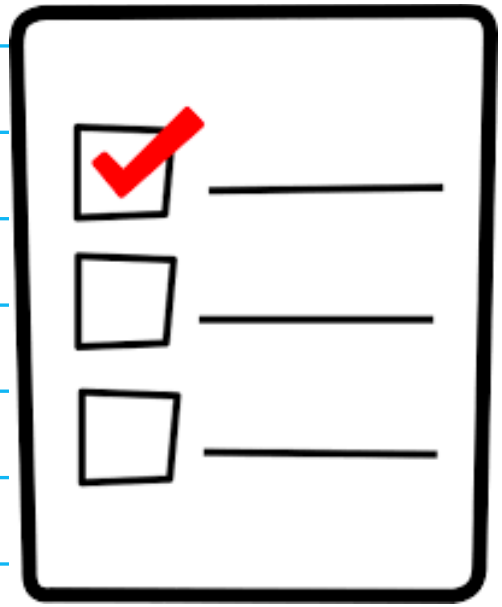
E-TICKETING

E-Ticket: contrato entre un usuario y un proveedor de servicios ...

… términos y condiciones.

E-TICKETING

INFORMACIÓN INCLUIDA EN EL TICKET



- Número de serie
- Emisor
- Prestador de servicios
- Usuario
- Servicio
- Términos y condiciones
- Tipo de e-ticket – Transferibilidad + Reusabilidad
- Atributos (p.e. número de asiento, destino del transporte, …)
- Tiempo de validez
- Fecha de emisión
- Campo que pruebe la identidad del emisor (firma digital)

E-TICKETING

REQUISITOS DE SEGURIDAD

- Integridad
- Autenticidad del emisor del ticket
- No repudio de origen
- No repudio de recepción
- Infalsificabilidad
- …

E-TICKETING

REQUISITOS DE SEGURIDAD

- ...
- Equidad
- No sobreutilización
- Reusabilidad
- Exculpabilidad
- Transferibilidad

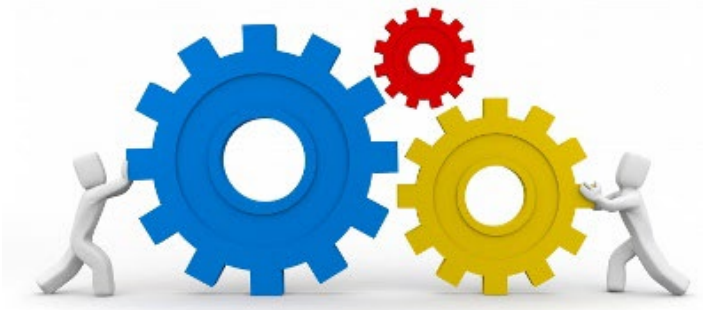
E-TICKETING

REQUISITOS DE PRIVACIDAD

e-tickets identificados	• la identidad del propietario debe ser verificable
e-tickets anónimos	• el propietario debe permanecer anónimo
Anonimato totalmente revocable	• la identidad del usuario está incrustada (de alguna manera) en los e-tickets • solo un reducido subconjunto de actores puede revelarla
Anonimato revocable selectivo	• la identidad de un usuario *fraudulento* de un e-ticket, a priori anónimo, puede ser revelada

E-TICKETING

REQUISITOS FUNCIONALES



Tiempo de validez	Verificación offline	Portabilidad
Tamaño reducido	Flexibilidad de uso en múltiples entornos	Facilidad de uso
Eficiencia	Flexibilidad de pago	...

Análisis de la aplicabilidad de los NFTs en sistemas de e-ticketing

Análisis de la aplicabilidad de los NFTs en sistemas de e-ticketing

Información incluida en el ticket NFT

Se puede almacenar en los *metadatos* asociados al NFT.

Se puede incluir en los metadatos un *puntero* a la ubicación de los datos *off-chain*.

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Cumplimiento de las propiedades de seguridad

Integridad

- los sistemas de gestión de NFTs son en esencia aplicaciones descentralizadas → inmutabilidad.

Autenticidad

- garantizada por la estandarización (cada token es identificable).

No repudio de origen ni de recepción

- las transferencias se registran en la blockchain.

Infalsificabilidad

- viene dada por la transparencia de blockchain.

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Cumplimiento de las propiedades de seguridad

No sobreutilización

- cuando un usuario transfiere un NFT deja de ser su propietario.

Exculpabilidad

- cuando un usuario utiliza un NFT, puede mantener la propiedad del NFT, que ahora estará marcado como *usado*.

Reusabilidad

- la sobreescritura de las funciones del token ERC-721 permitiría contadores de control de la reusabilidad del token.

Transferibilidad

- solo el propietario de un NFT puede transferirlo (ERC-721 define la propiedad).
- Puede interesar contar con NFTs no transferibles - **Soulbound tokens (**SBTs).

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Cumplimiento de las propiedades de privacidad

Identificación del usuario del servicio

- en el caso de tickets identificados la identidad del usuario debe incluirse en el NFT.

Anonimato

- aunque la identidad del usuario puede no formar parte del NFT, este está vinculado a la dirección de su propietario → el anonimato NO puede ser fuerte.

Anonimato revocable general

- debería contar con un mecanismo para obtener las identidades de todos los propietarios.

Anonimato revocable selectivo

- debería permitir la revocación únicamente de los usuarios fraudulentos.

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Cumplimiento de las propiedades de privacidad

Identificación del usuario del servicio

- en el caso de tickets identificados la identidad del usuario debe incluirse en el NFT.

Anonimato

- aunque la identidad del usuario puede no formar parte del NFT, este está vinculado a la dirección de su propietario → el anonimato no puede ser fuerte.

Anonimato revocable general

- debería contar con un mecanismo para obtener las identidades de todos los propietarios.

Anonimato revocable selectivo

- debería permitir la revocación únicamente de los usuarios fraudulentos.

La gestión del anonimato y su revocación no están resueltas en los NFTs.

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Cumplimiento de las propiedades funcionales

Tiempo de validez

- Puede aparecer entre los datos del NFT.

Verificación on-line/off-line

- Debería realizarse on-line → tiempos de espera.

Portabilidad

- No requieren ser transportados en un dispositivo.

Tamaño reducido

- De los tokens y de los contratos - asociado a los costes.

Flexibilidad

- Es una de las potencialidades de los NFTs.

Facilidad de uso

- Las herramientas de gestión no son todavía de uso extendido.

Análisis de la aplicabilidad de los NFTs en sistemas de e-ticketing

Retos inherentes al uso de NFTs

Coste

- *Ethereum - tarifa de gas*: para realizar cualquier transacción.

Ataque del 51 por ciento

- Poco probable debido a la descentralización.

Propiedad intelectual

- Debe incluirse entre los metadatos del contrato inteligente subyacente.

Ciberseguridad

- Criticidad de la seguridad de los contratos inteligentes.

Impacto ambiental

- Potencial influencia en el calentamiento global.

Análisis de la aplicabilidad de los NFTs en sistemas de e-ticketing

Retos inherentes al uso de NFTs

Privacidad

- Identidades.
- Información confidencial de los activos digitales.

Usabilidad

- Falta de interfaces fáciles de usar.

Mantenimiento

- Convivencia de NFTs con diferentes versiones de contratos inteligentes.

Extensión

- Los ecosistemas NFT existentes están aislados entre sí.

ANÁLISIS DE LA APLICABILIDAD DE LOS NFTS EN SISTEMAS DE E-TICKETING

Retos específicos de los NFTs usados en e-ticketing

Privacidad

- Tickets identificados:
  en un NFT se define al propietario → éste podría ser identificado.
  RETO: esta identificación debe ser correcta y segura.

- Tickets anónimos:
  RETO: cómo conseguir que no permitan identificar al usuario?

- La privacidad NO se garantiza en la blockchain (transparencia) → el anonimato es un desafío.

Análisis de la aplicabilidad de los NFTs en sistemas de e-ticketing

Retos específicos de los NFTs usados en e-ticketing

Adopción de la tecnología

- Fase inicial - problemas de adopción por los usuarios.

Limitación de la transferibilidad

- No se puede evitar que el titular venda un token, pero …
  … quedará constancia de la transacción.
- El contrato inteligente puede restringir el precio de reventa, pero …
  … no tiene control sobre los pagos en efectivo.
- Insignia: token que, una vez asignado, no se puede transferir.

Oportunidades

OPORTUNIDADES

REGALÍAS

- UN NFT PUEDE SER PROGRAMADO PARA PAGAR REGALÍAS A SU CREADOR CADA VEZ QUE SE VENDE A UN NUEVO PROPIETARIO.

PROPIEDAD FRACCIONADA

- Permite a diferentes usuarios poseer una parte de un NFT específico.

TICKETS COLECCIONABLES

- Después de ser usado, pueden pasar a formar parte de colecciones.

Conclusiones

CONCLUSIONES

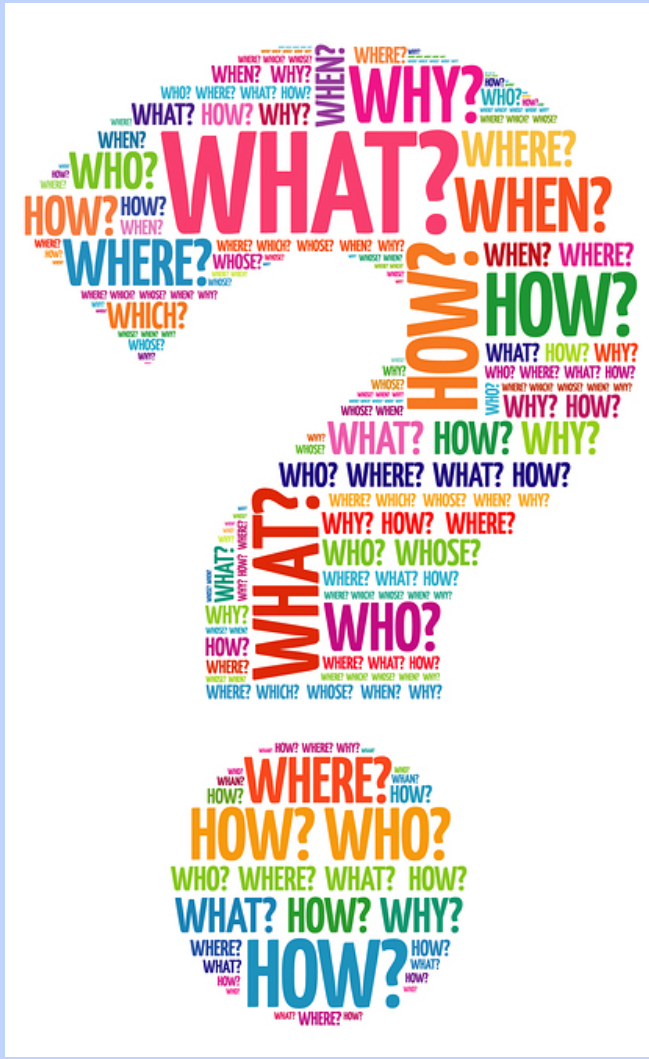
Los NFTs representan la singularidad, basándose en blockchain.

Los e-tickets mediante NFTs son un caso de uso viable.

Se han presentado los requisitos a satisfacer en un sistema de e-ticketing: Seguridad // Privacidad // Funcionalidad.

Se han evaluado dichos requisitos en el uso de NFTs para e-tickets, identificando los retos a afrontar.


Eskerrik
asko
Gràcies
DANKSCHEEN
BÏYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
GRACIAS
SUKSAMA
EKHMET
THANK
ARIGATO
SHUKURIA
MAAKE
GRAZIE
MEHRBANI
PALDIES
YOU
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
KOMAPSUMNIDA
BOLZÏN
MERCI


WHEN?
WHY?
WHERE?
WHO?
WHAT?
HOW?
WHICH?
WHOSE?