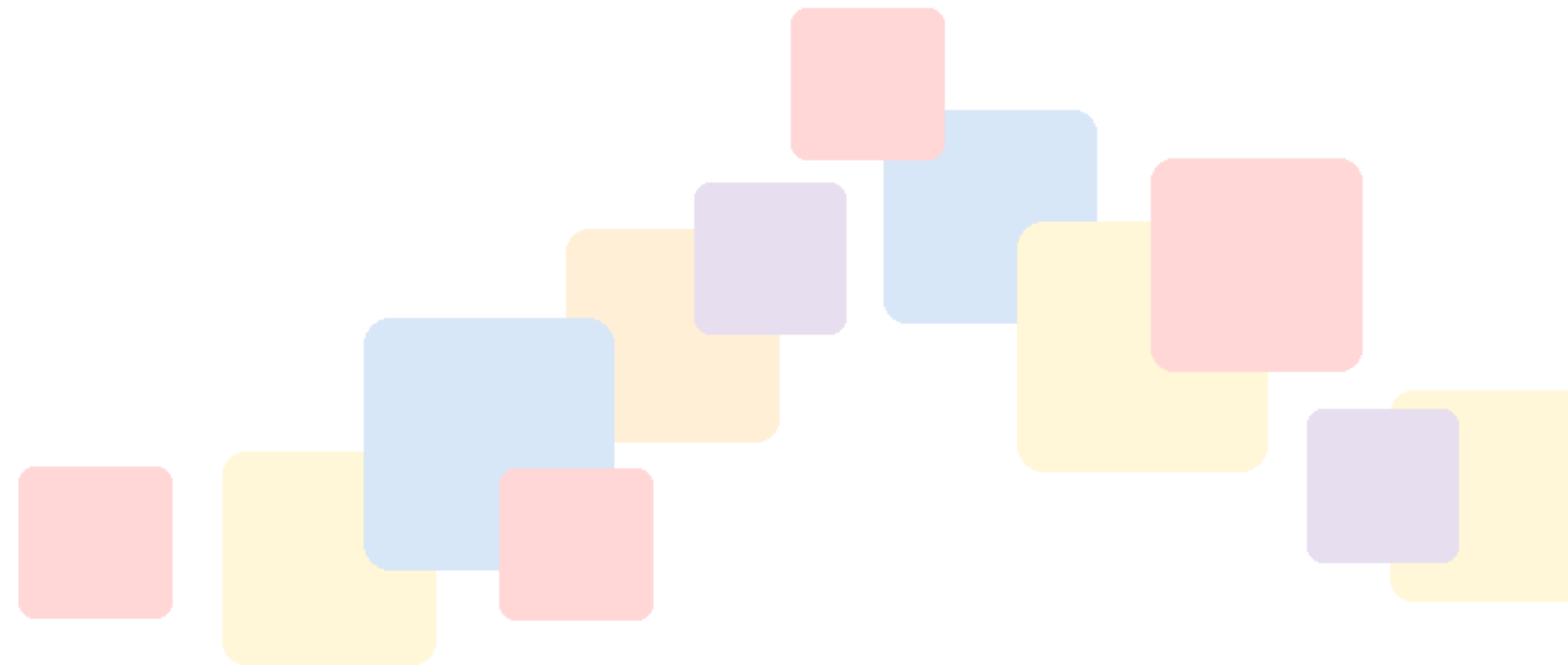


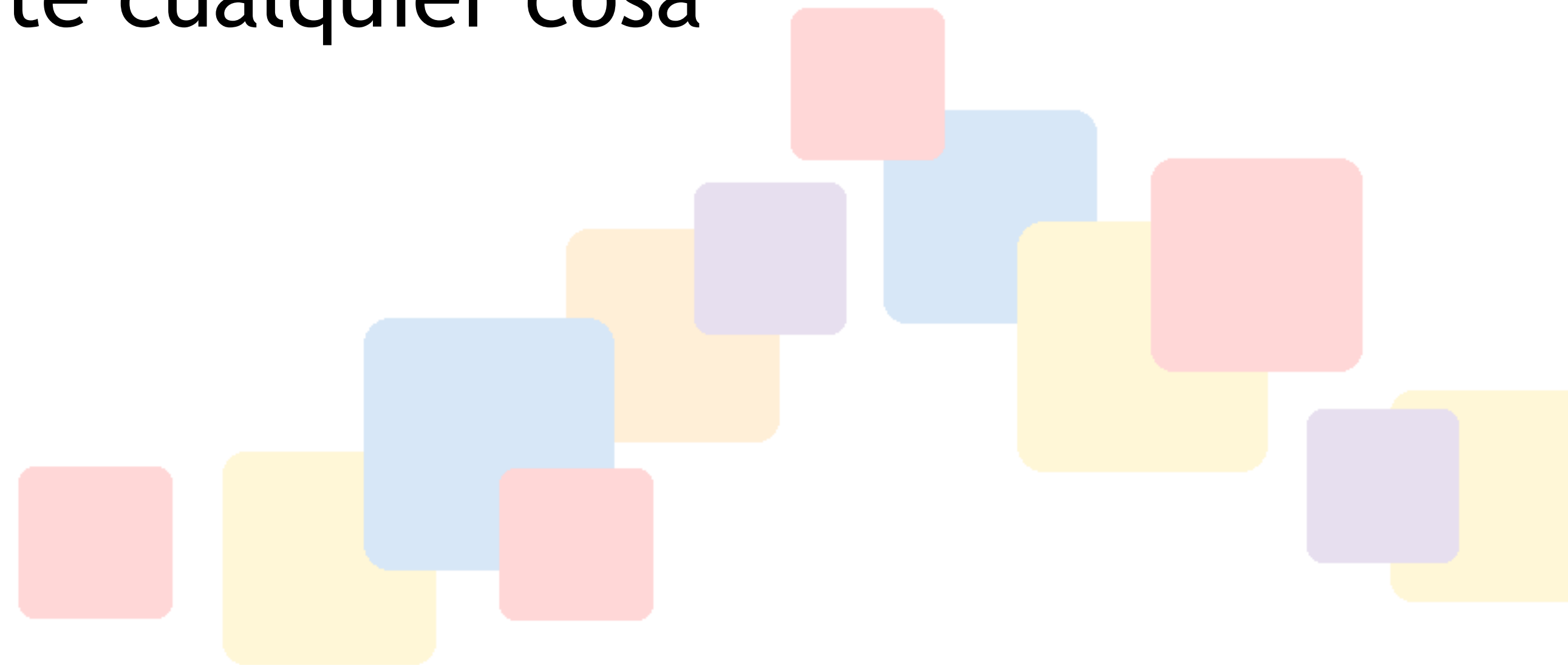
Clase 2: Tokens

Cliente: COPEC



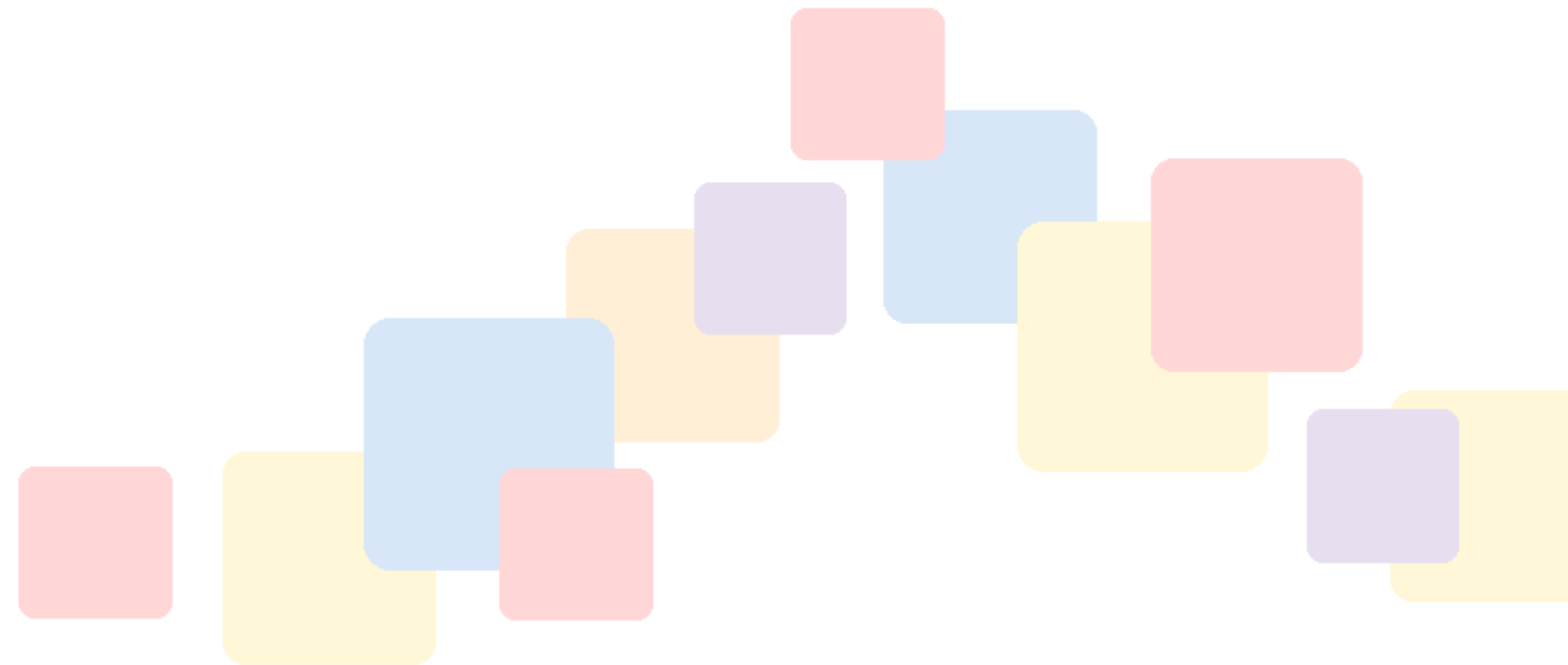
¿Qué es un Token?

- Es un activo digital
- Se pueden transar y mover fácilmente
- Pueden representar virtualmente cualquier cosa



Tipos de Tokens

- Fungibles
 - Lo que representan es “intercambiable” entre si
 - Ejemplo por antonomasia es el dinero
- No Fungibles
 - Representan algo único
 - Una persona, por ejemplo



Qué cosas pueden representarse con Tokens Fungibles

- Dinero
- Acciones de una misma serie
- Cajas de Productos Comestibles (Clamshell de Arándanos)
- ¿Litros de Combustible?



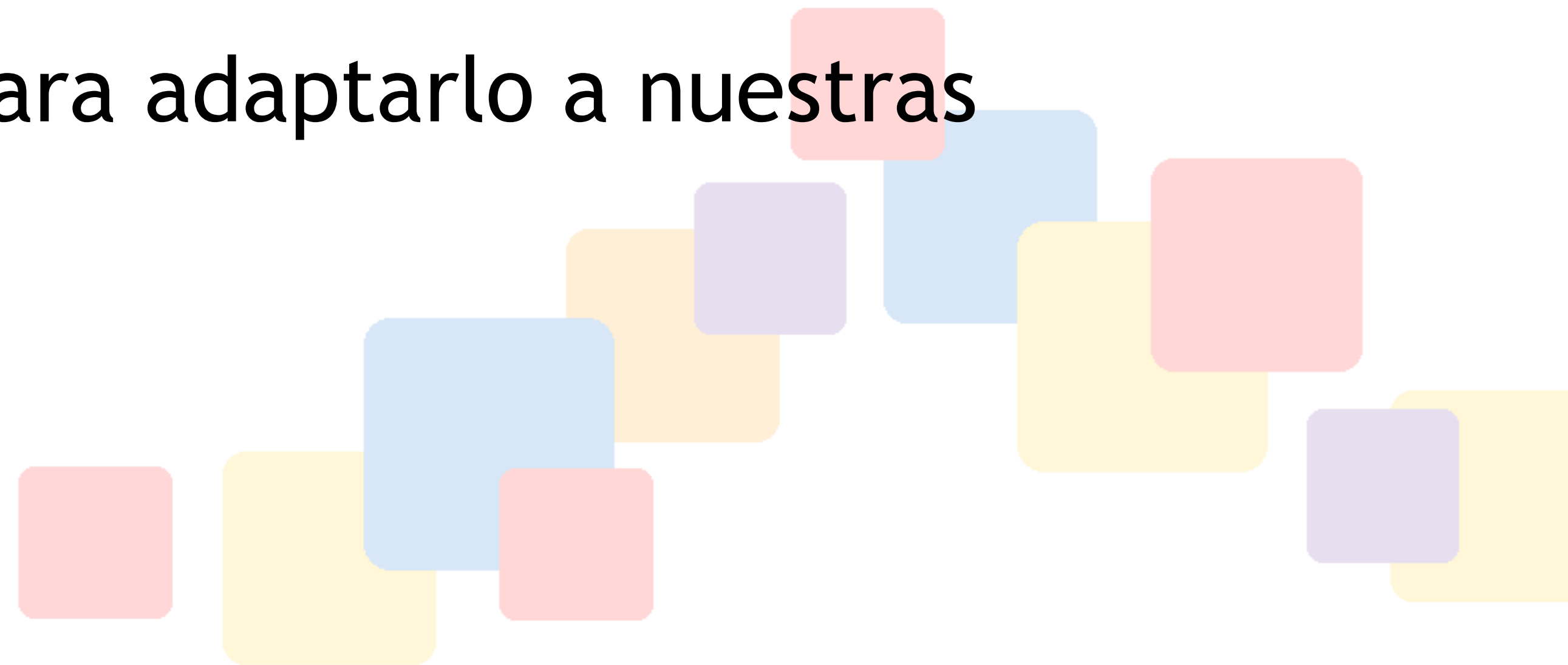
Qué cosas pueden representarse con Tokens No Fungibles

- Identidad de Personas
- Entradas numeradas a un evento
- Obras de Arte
- Membresías de Participación

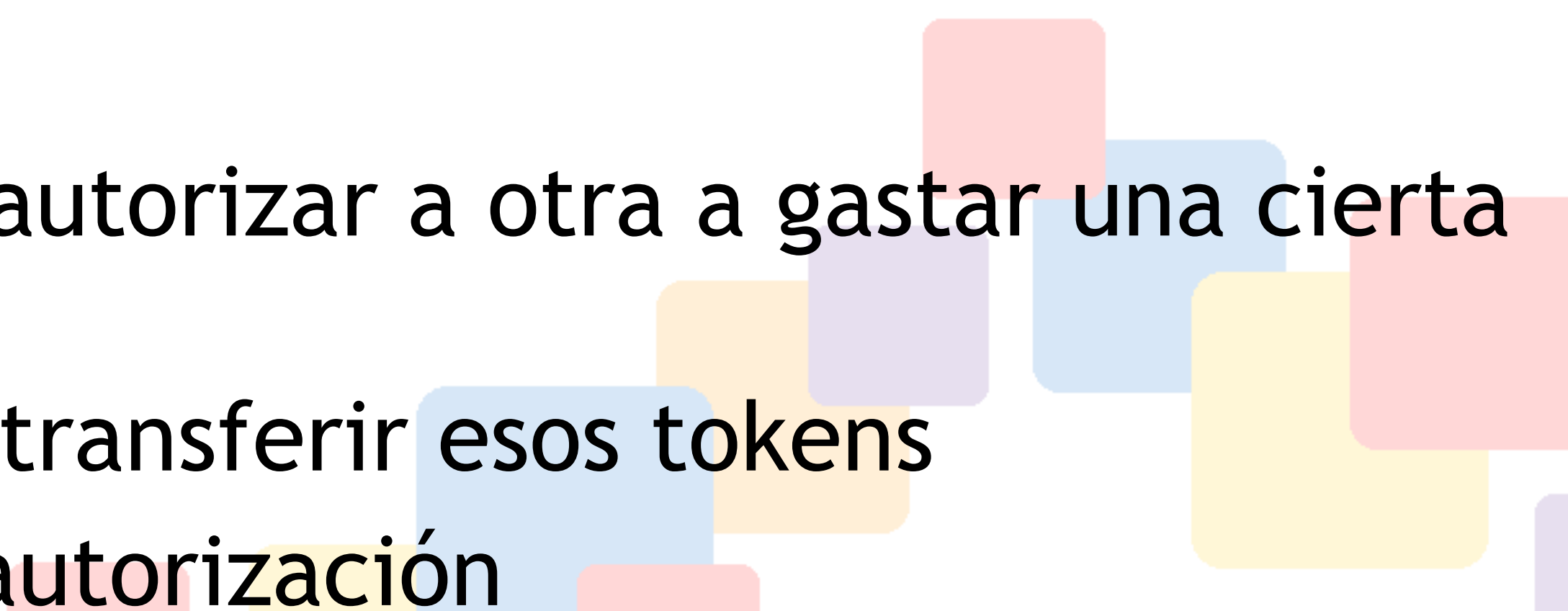


Estándar ERC20

- Estándar del token fungible
- Exige la implementación de ciertos métodos y una funcionalidad básica
- Esta puede extenderse luego para adaptarlo a nuestras necesidades



Qué debe hacer un token ERC20

- Consultar el saldo de una billetera
 - Permitirle al dueño de la billetera transferir sus tokens a otra persona
 - Conocer el total de tokens en circulación
 - Permitir al dueño de una billetera autorizar a otra a gastar una cierta cantidad de sus tokens
 - Permitir al que está autorizado transferir esos tokens
 - Permitir al dueño revocar esta autorización
- 

Funcionalidades adicionales

- Acuñar más tokens
- Quemar tokens
- Restringir quien puede recibir tokens
- Pedir una autorización sobre ciertos montos transferidos
- Etc.



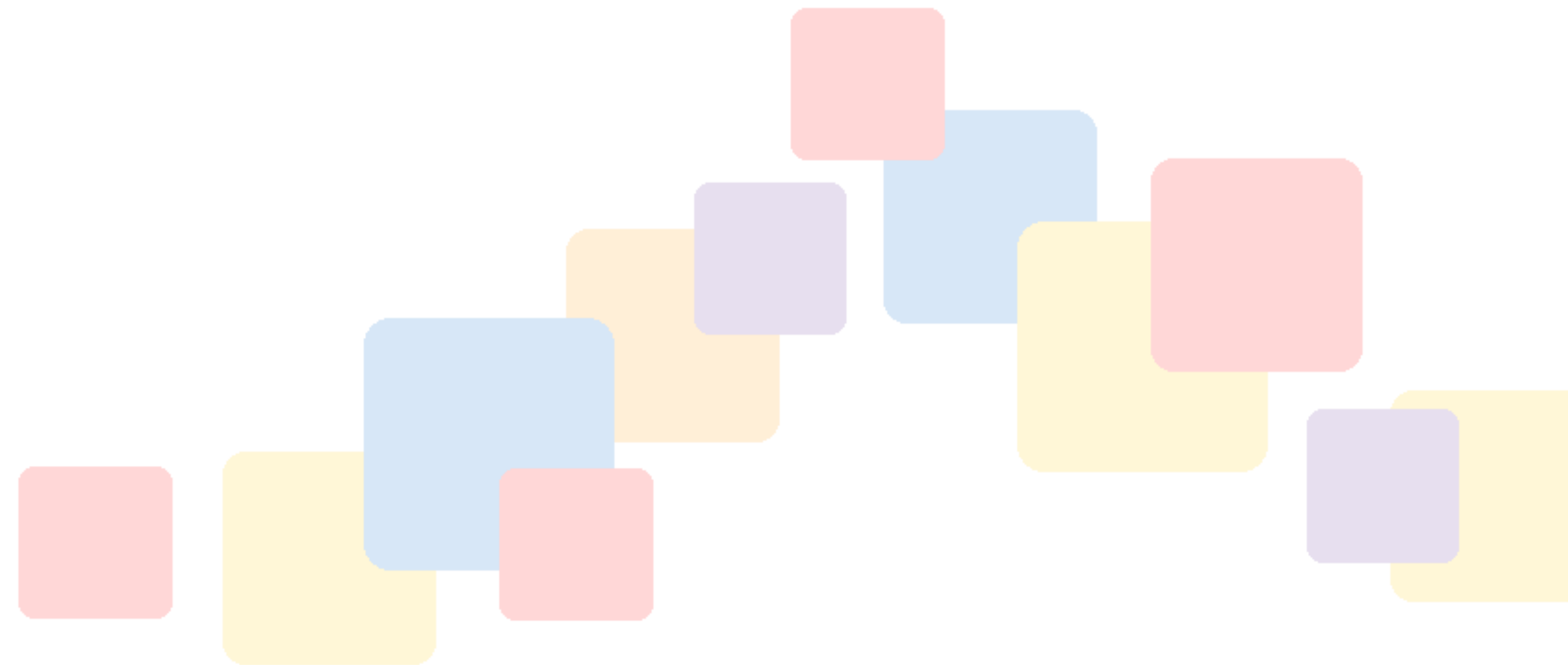
Estándar OpenZeppelin

- Implementación de Token ERC20 referencial
 - “Battle Tested”
 - Muy simple de usar
 - Extensible
 - Muy robusta
 - Auditada
 - Pese a eso, se usa bajo el propio riesgo
- Forma más rápida de usar
 - <https://wizard.openzeppelin.com/>



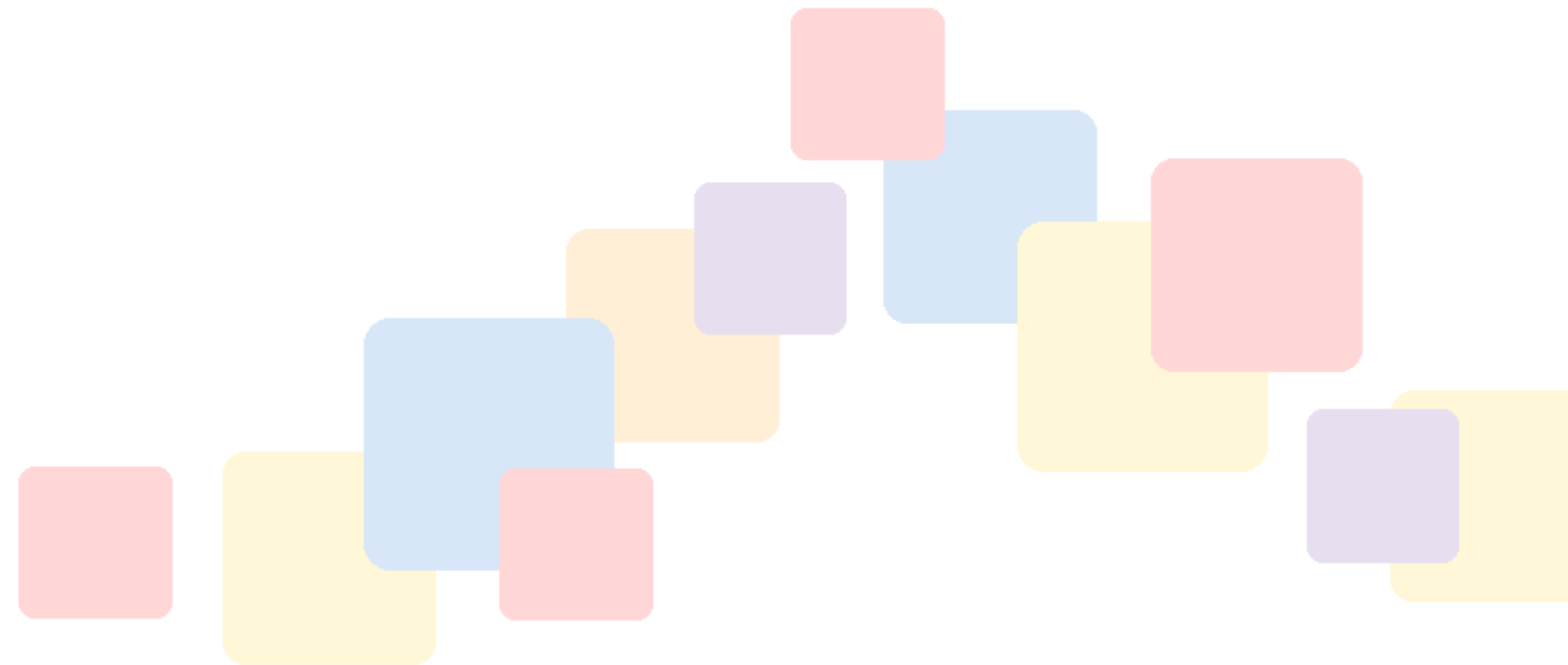
NFTs - Estándar ERC721

- Define las operaciones “básicas” de un token no fungible
- Dado que la naturaleza implica representar algo off chain, parte de la data se guarda fuera de la cadena
-



Puntos Principales del ERC721

- Verificar Propiedad
- Transferir
- Autorizar a transferir
- URL para obtener Metadata



Metadata

- Archivo JSON
- Nombre, imagen, descripción y otros
- Se puede almacenar en cualquier parte
 - IPFS si quieres que sea inmutable
 - Cualquier sistema si necesita mutar
 - Complementado con Hash si hace falta...



HashLocked Contracts

- Consisten en “Liberar” una transacción de un contrato pidiendo que se revele un secreto
 - Este secreto tiene la forma de la preimagen de un hash
- Se utiliza el mismo hash del secreto, en dos contratos independientes que se quiere enlazar
 - Típicamente, en dos redes diferentes



Ejemplo

SBF



Tengo AVAX
Quiero MATIC

CZ



Tengo MATIC
Quiero AVAX

Ninguno de los dos confía en el otro....



Proceso (muy simplificado)

- SBF selecciona una frase al azar y calcula su hash
- SBF crea un hashlocked contract y deposita los AVAX que quiere vender
 - Usa como parametro el hash del secreto que calculó y el address de CZ
- CZ crea un contrato análogo, con los MATIC que quiere vender
 - Usa el mismo hash de SBF (si no confía, puede verificar el comprobante) y el Address de SBF
- SBF usa el secreto para retirar los MATIC.
- CZ usa el mismo secreto para retirar los AVAX. Si SBF no lo entrega, puede ver lo comprobantes

