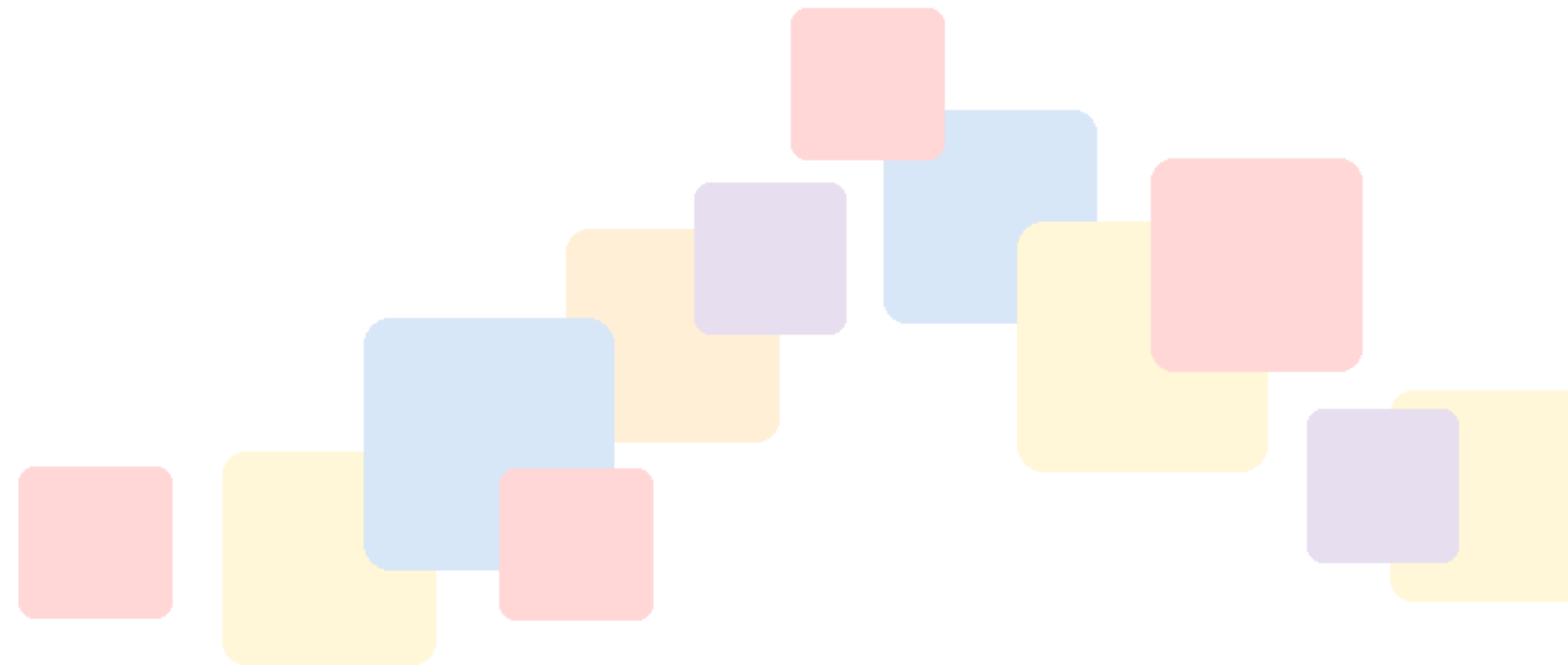


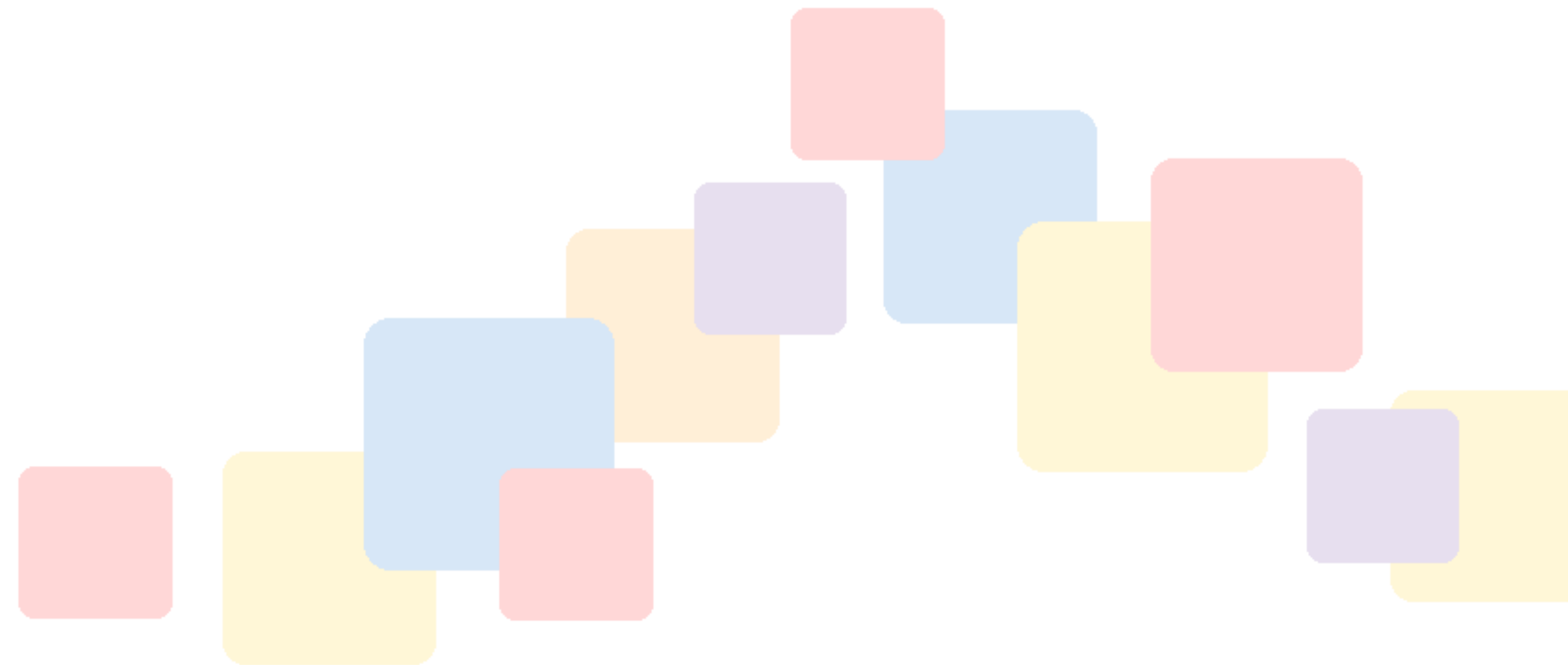
Clase 3: Smart Contracts

Cliente: COPEC



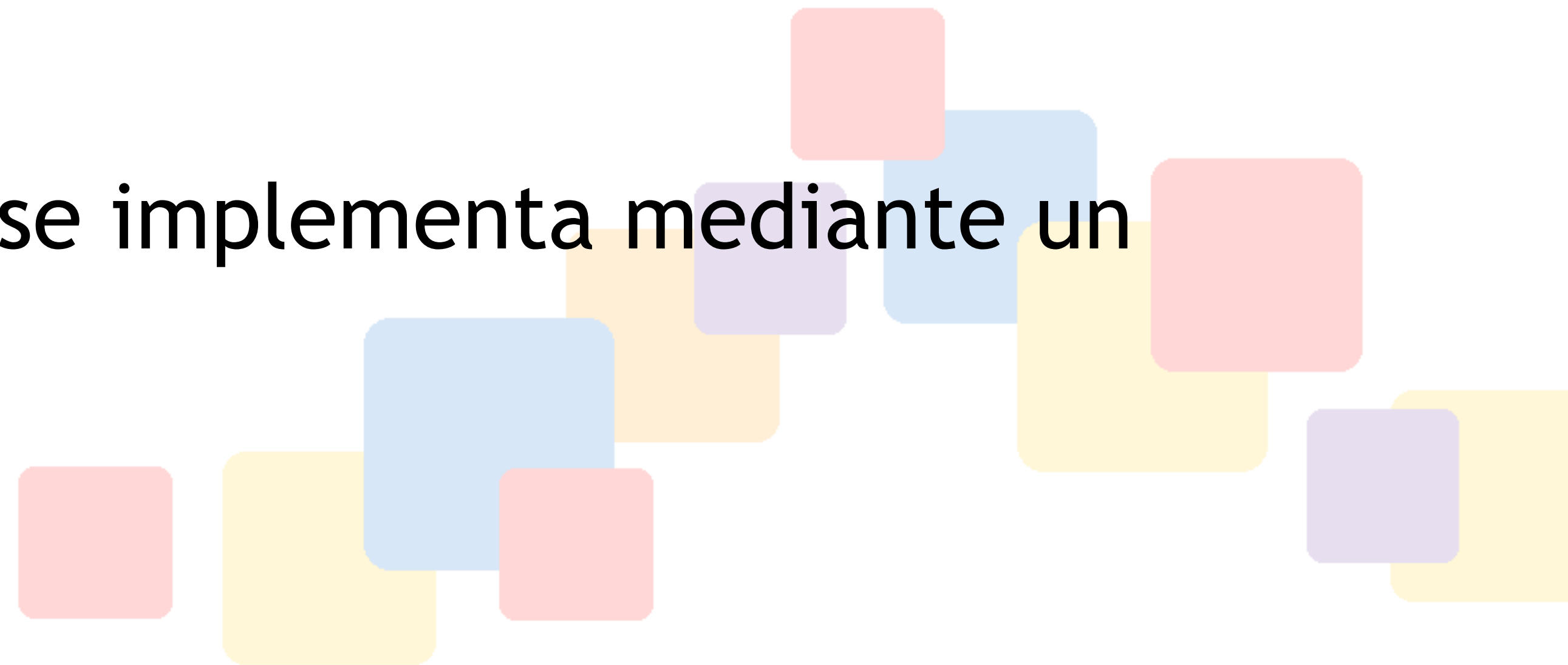
Temas de Hoy

- Multifirmas
- OpenZeppelin Defender
- DAOs
- HardHat



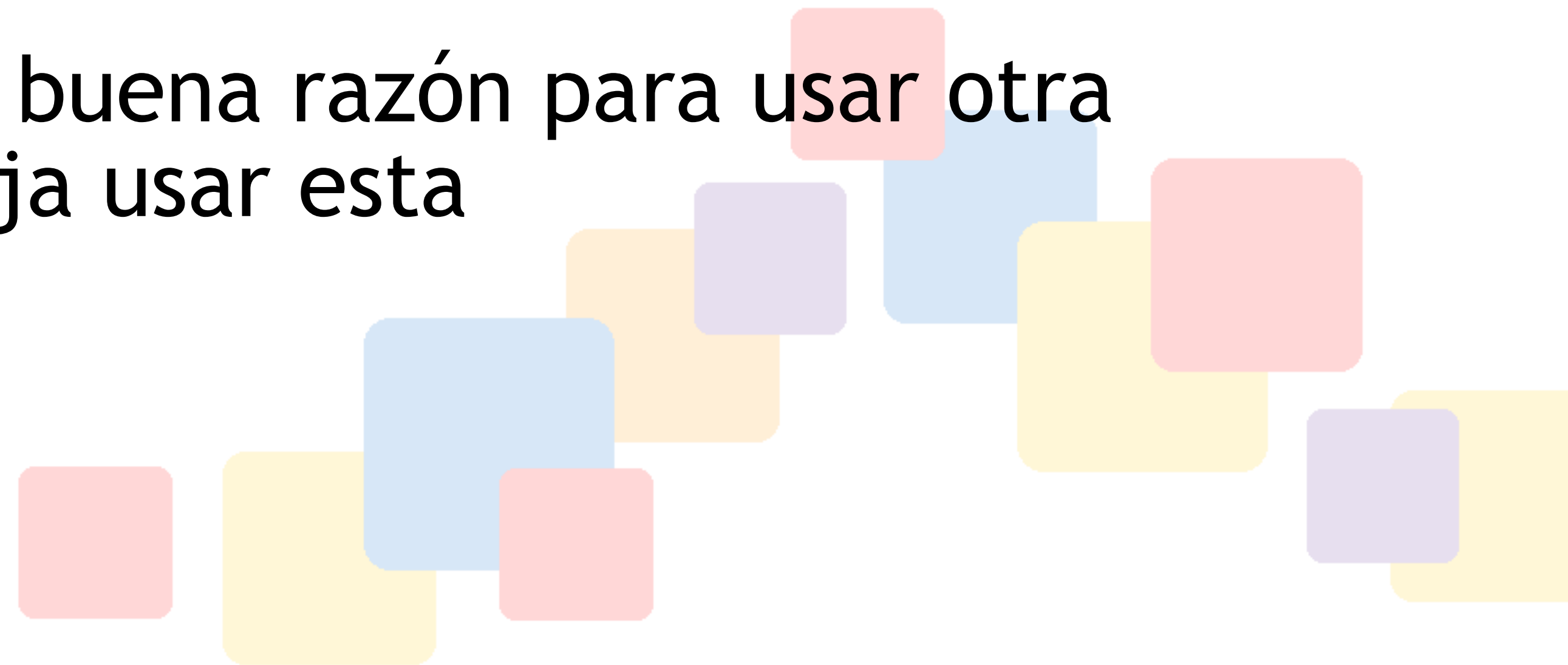
Billeteras Multifirmas | Smart Contract Wallet

- Permiten ejecutar una transacción sujeta a más de una firma criptográfica
- En Bitcoin, operan en forma nativa
 - Schnorr
- En las redes EVM compatibles, se implementa mediante un Smart Contract



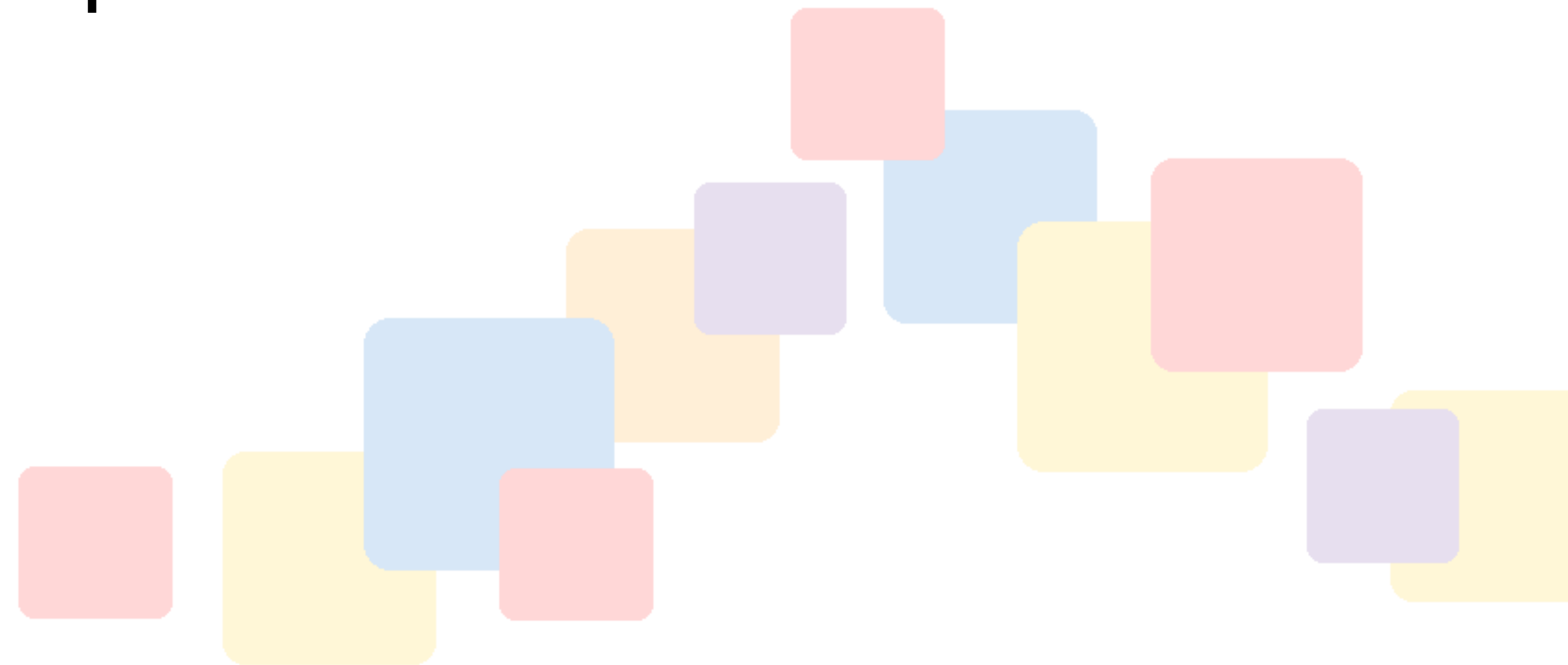
Gnosis Safe

- Partió como parte de un proyecto de Mercados Predictivos
- Se convirtió en el estándar de facto de las billeteras multifirmas
- A menos que se tenga una muy buena razón para usar otra billetera multifirma, se aconseja usar esta



Ventajas

- “Battle Tested”
 - Muy probada y auditada
 - Custodia cientos de millones de dólares en cripto
 - Hay un contrato con USD10MM de premio: si lo hackeas, son tuyos.... Hasta ahora nadie ha podido
- Disponible en múltiples redes
- Open Source
 - Instalable en redes privadas



Ejemplos Prácticos

- Crear una billetera Multisig
- Hacer una transferencia de Fondos
- Llamar a un contrato inteligente



OpenZeppelin Defender

- Herramienta de Administración de Smart Contracts
 - Remix es bueno para desarrollar, pero pobre para administrar
- Desarrollado por uno de los referentes de la industria
 - Difícil que otra empresa lo implemente mejor
- Dispone de una capa de uso gratuita



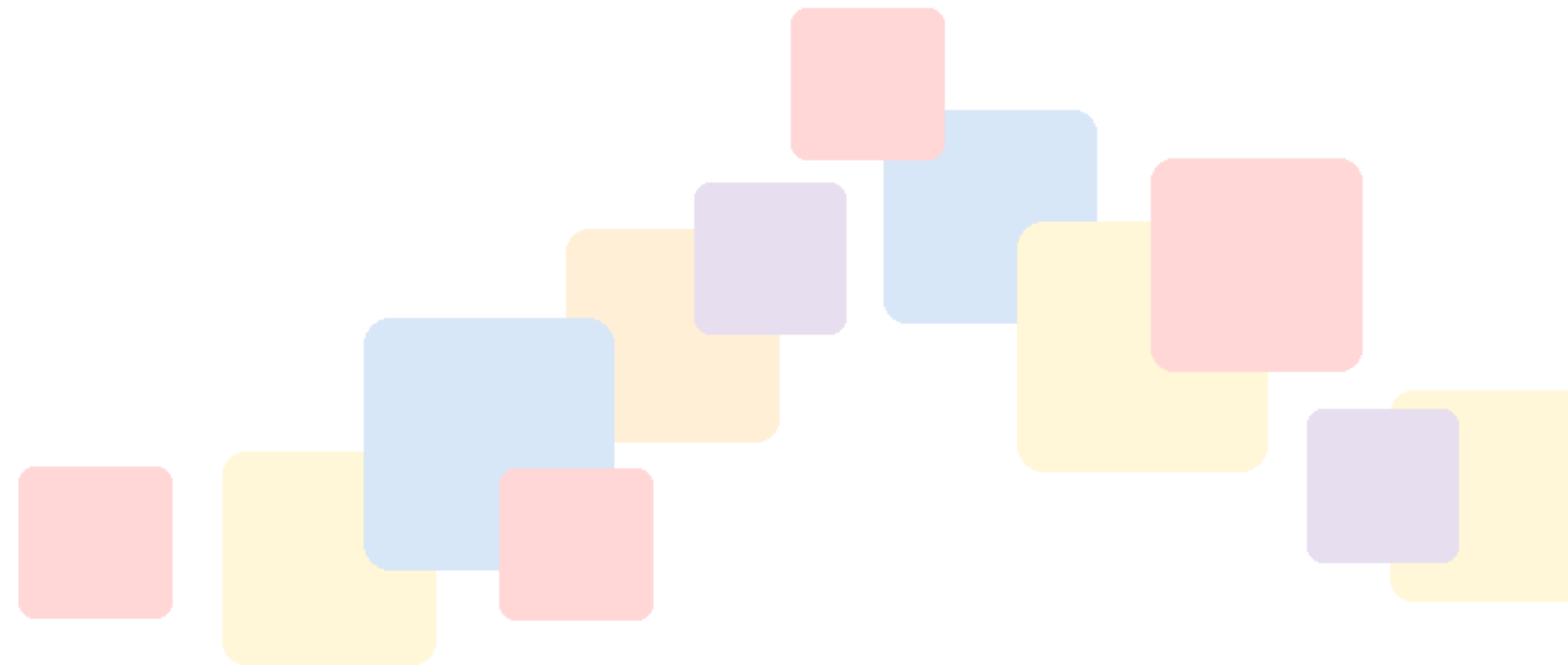
Funcionalidades

- Administrar Smart Contract
 - Dígase llamar funciones
- Llamar un contrato inteligente medianter API
 - Relayer
- Invocar un contrato a intervalos regulares
- Monitorear la actividad de un contrato



Ejemplos Prácticos

- Crear un admin en Defender
- Crear un Timelock
- Administrar con una Safe
- Crear una alerta con Sentinel



DAOs

- Decentralized Autonomous Organization
- Hay muchas formas de definirla, la que más me gusta
- Mecanismo para dar gobernanza descentralizada a cualquier proyecto blockchain público
 - También tienen sentido para proyecto basados en blockchain privados



En que consisten

- Mecanismo de distribución del poder de voto
 - Token ERC20
 - NFT
 - Delegación
- Se administran
 - Decisiones sobre un Smart Contract
 - Tesorería
 - Control de un canal de comunicación (Slack, Discord, etc)



Ejemplo Práctico

- Votación con Snapshot



Hardhat

- Toolbox de desarrollo de Smart Contracts
- Facilita y automatiza muchas tareas como
 - Probar Smart Contracts
 - Procesos de Despliegue
 - Verificación de Código

