

# Clase6



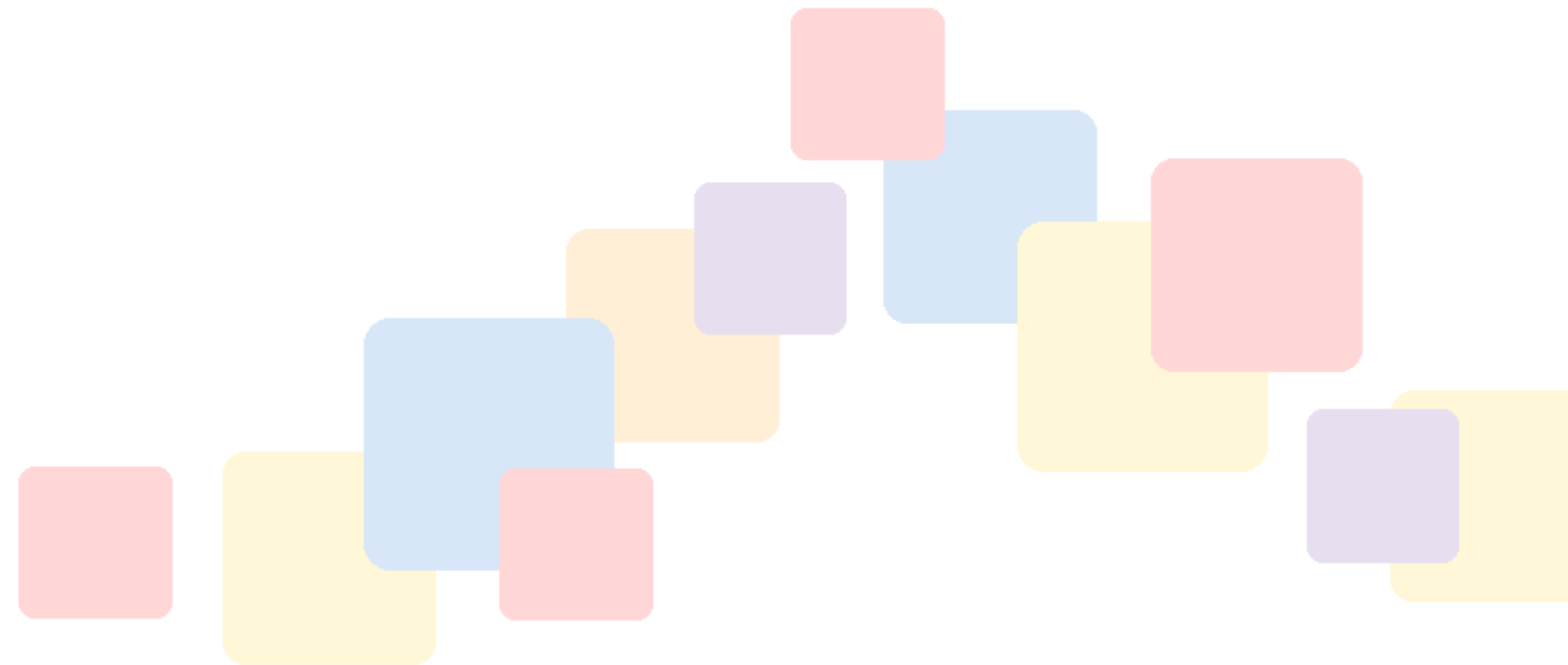
# Pruebas de Conocimiento

## Cero



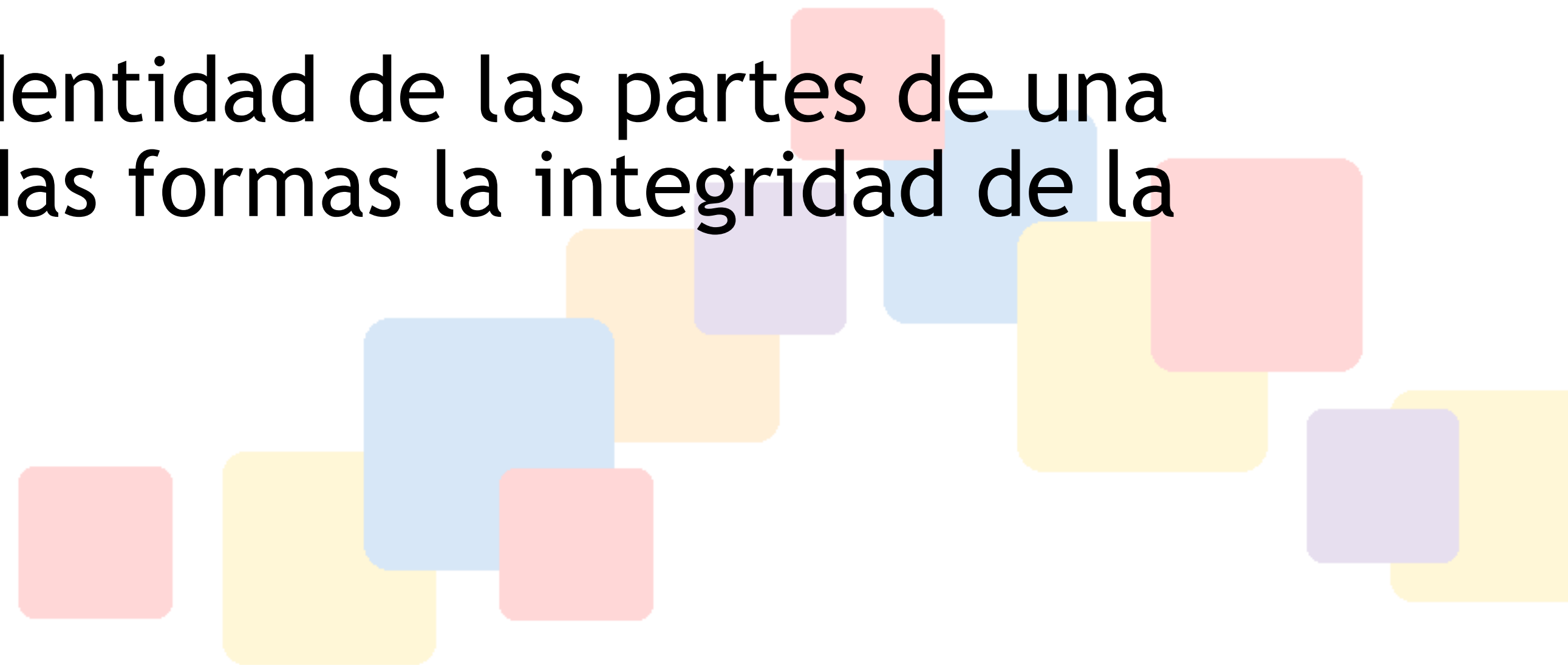
# Disclaimer

- Matemáticas detrás de esto son muy complejas
- Recién en 2015 aparecieron formas relativamente viables de hacer esto



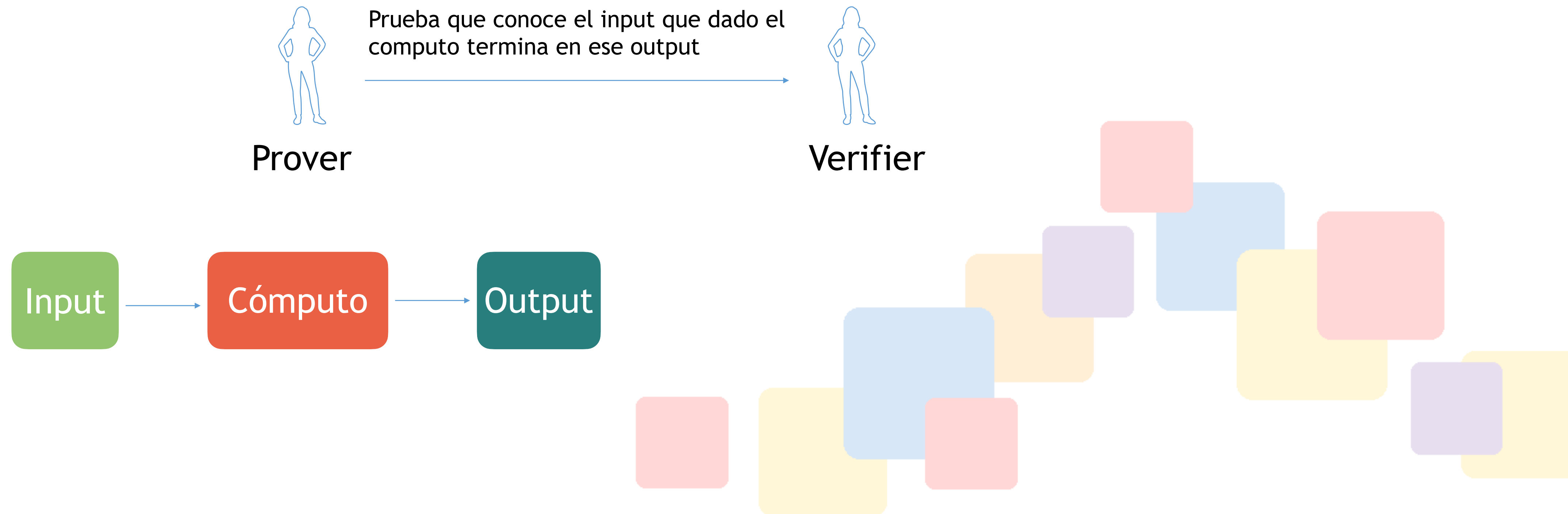
# Monero

- Primera criptomoneda en usar los ZK Snarks
- Primer caso practico de uso de pruebas de conocimiento cero no interactivas
- Permiten mantener oculta la identidad de las partes de una transacción, asegurando de todas formas la integridad de la data



# ZK Snarks

- Zero Knowledge Succinct Non Interactive Argument of Knowledge



# ZK Snarks: Pasos

1. Representar el cálculo computacional en forma de restricciones entre variables
2. Reducir estas restricciones a un conjunto de ecuaciones polinómicas
3. Elegir un valor aleatorio y un mapeo irreversible de este y todas las ecuaciones a un espacio homomórfico, basado en matemáticas de curva elíptica (no me pregunten...)
  1. Básicamente, las ecuaciones originales se siguen cumpliendo (sumas y multiplicaciones)
  2. No se puede calcular el original a partir del mapeo
  3. “Encripta” las ecuaciones

Nota: bajo criptografía homomórfica, las operaciones de adición y multiplicación sobre valores encriptados siguen cumpliendo



# Criptografía Homomórfica

$$x + y = z$$

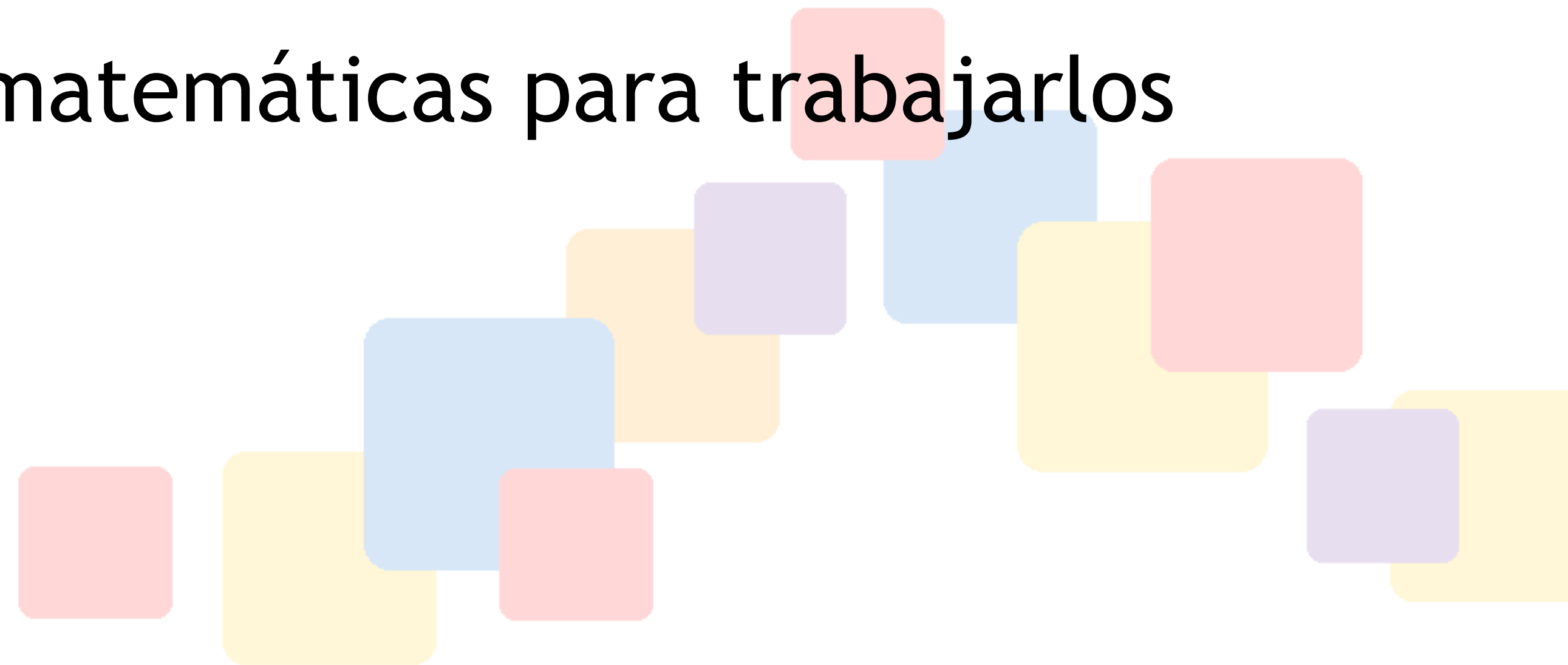
$$f(x) + f(y) = f(z)$$

$$f(x) \times f(y) = f(z)$$



# Porqué se hace esta reescritura

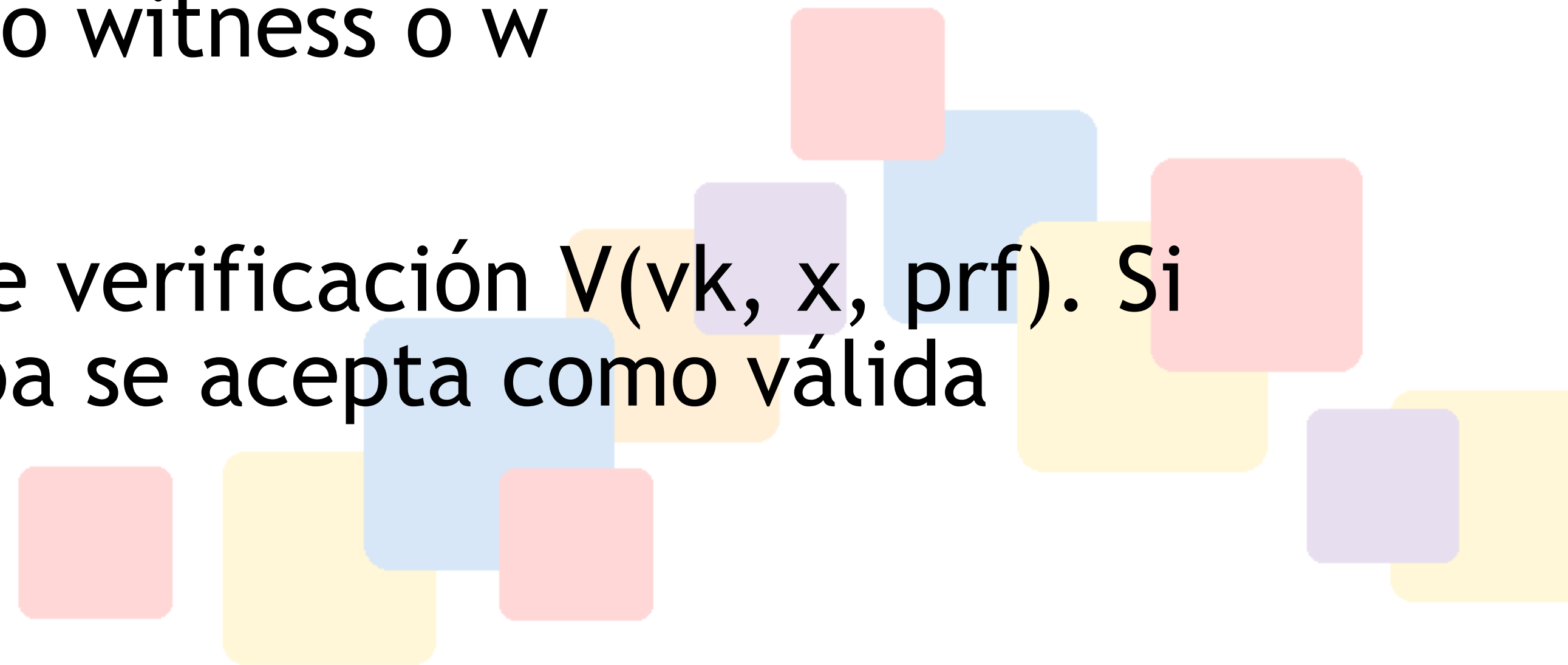
- No hay forma de codificar homomórficamente el cálculo computacional
- Sí lo hay para los polinomios
  - Pueden manejar mucha información
  - Hay siglos de herramientas matemáticas para trabajarlos





# Zk Snarks

- A partir de esto:
  - Key generator: recibe un parámetro secreto  $\Lambda$  (el secreto del paso 3) y genera dos llaves públicas: proving key (pk) y verification key (vk)
  - Prover genera una prueba prf, que es función de la proving key, el output  $x$ , y un secreto witness  $w$
  - $\text{prf} = P(\text{pk}, x, w)$
  - Verifier calcula la función de verificación  $V(\text{vk}, x, \text{prf})$ . Si esta devuelve true, la prueba se acepta como válida



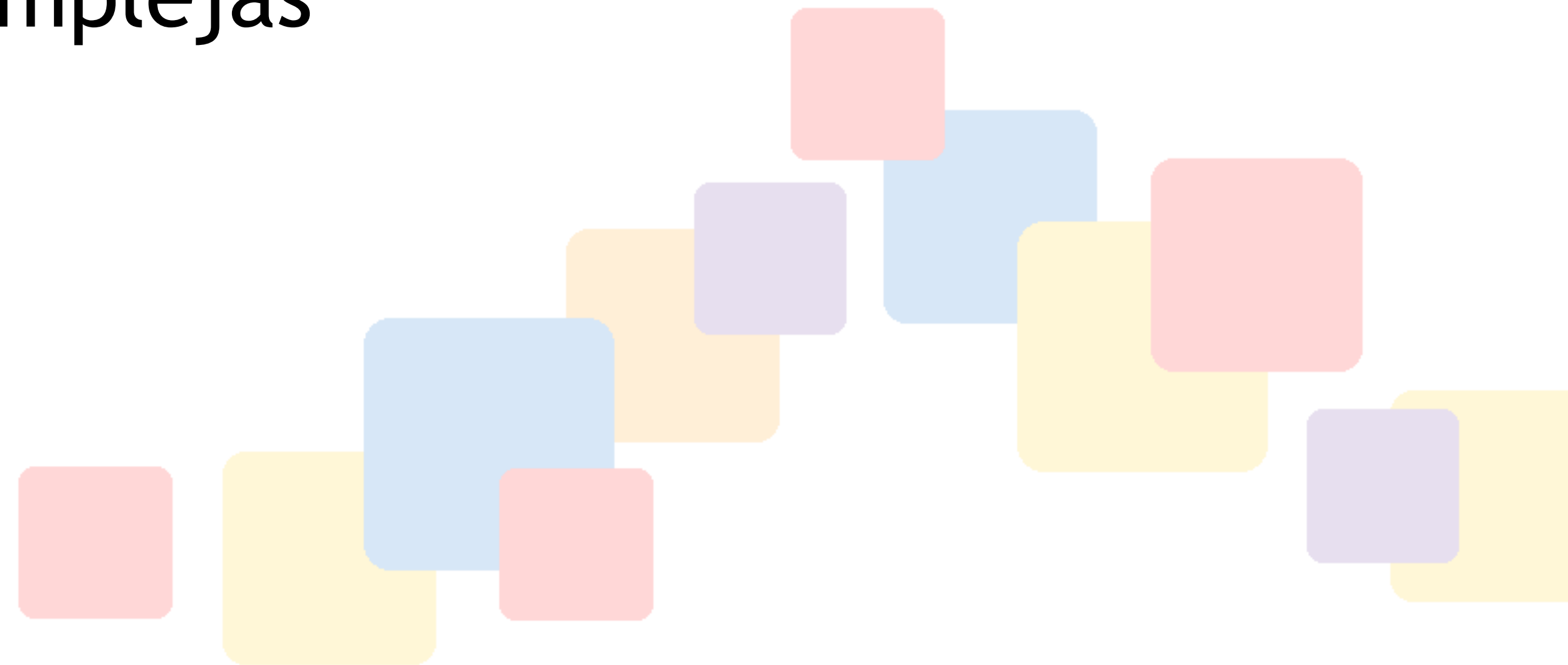
# ZK Snarks

- Se deben generar llaves  $pk$  y  $vk$  para cada proceso de cómputo en forma separada
- El parámetro  $\Lambda$  debe ser secreto. Si es conocido por alguien, este puede generar pruebas falsas
  - Es muy difícil asegurar que nadie lo conoce
- Ceremonia de ZCash
  - Múltiples testigos
  - Computadores con el WiFi y bluetooth físicamente destruidos
  - Etc




# Variaciones y mejoras

- Existen diversas formas de implementar esto
- Variadas funciones que “encriptan” los polinomios
- Ceremonias de setup menos complejas

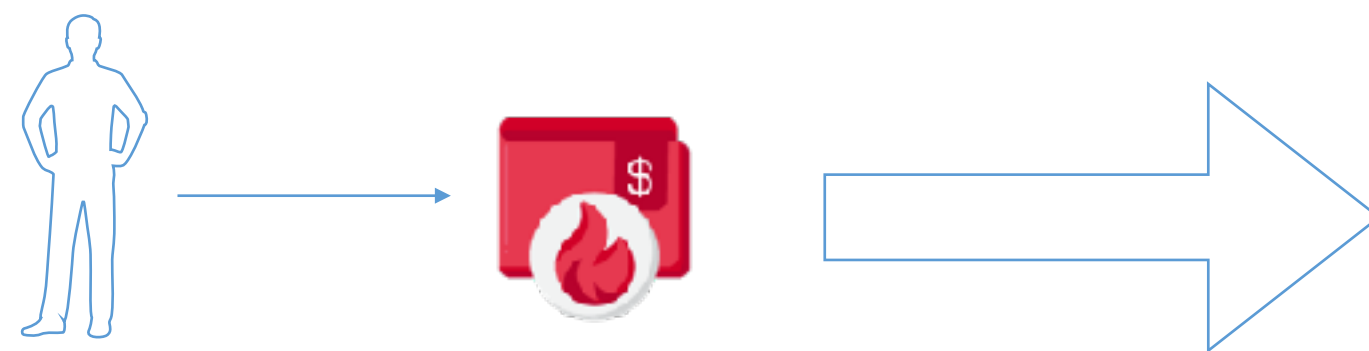


# Plonk

- Permutations over Lagrange-bases for Oecumenical Noninteractive Arguments of Knowledge
    - El proceso de trusted setup es, hasta ciertos límites, reutilizable
    - Pueden participar muchas personas, basta que uno sea honesto para que el proceso funcione
  - Usan una técnica llamada “polynomial commitments”, pero pueden cambiarse por otras técnicas criptográficas
  - La transformada de Fourier puede hacerse homomórfica y puede usarse en este proceso también
- 

# AZTEC y zk..money

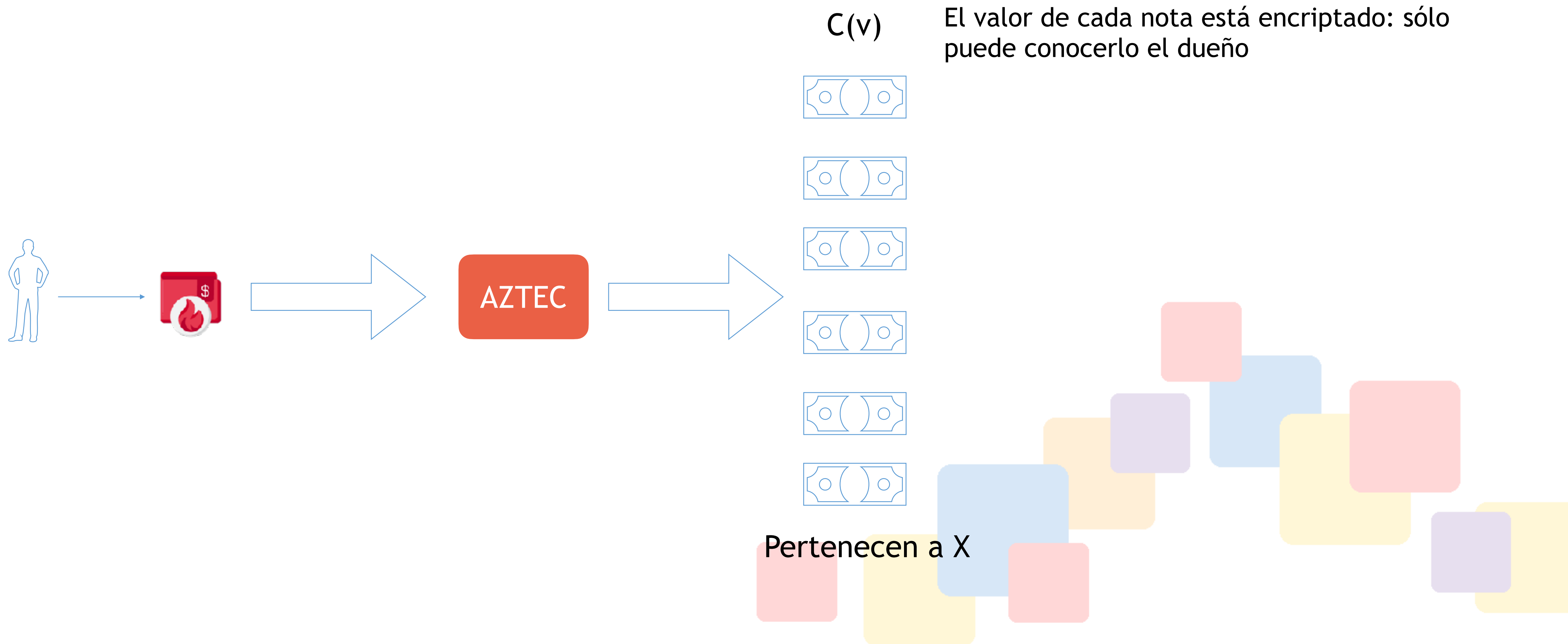
- Se basa en un sistema de Unspend Transaction Output, similar al del Bitcoin, combinado a un árbol de Merkle



Saber todas las transacciones

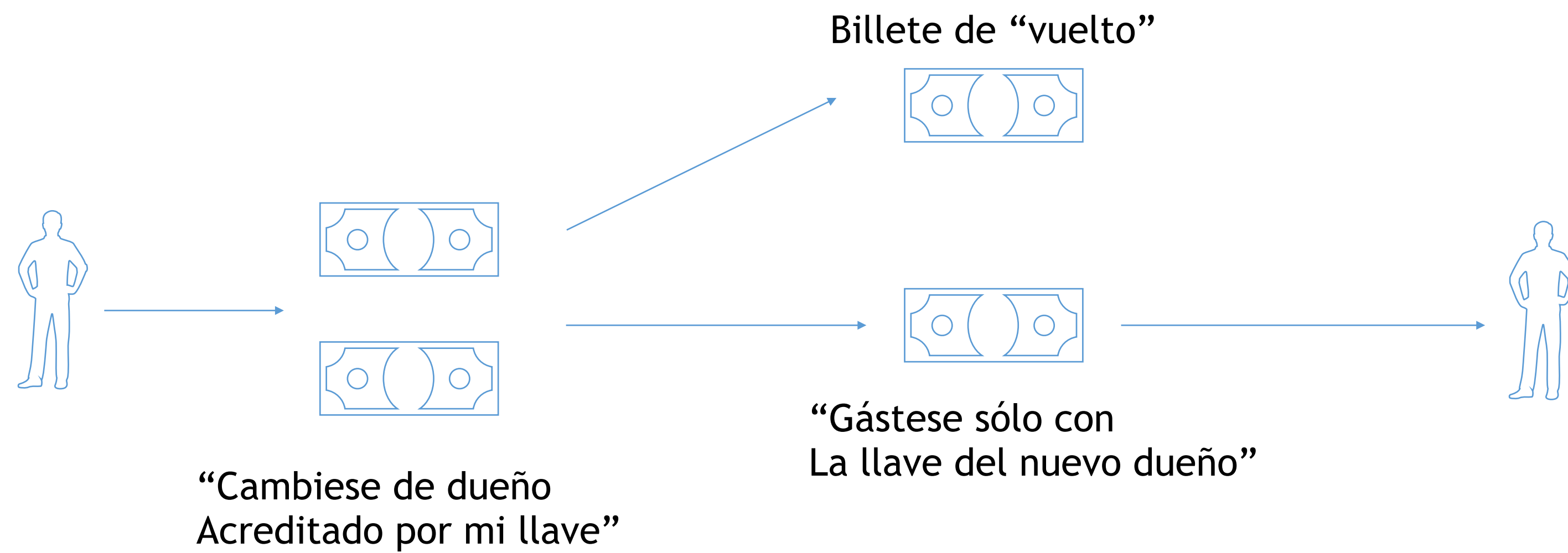


# AZTEC y zk..money



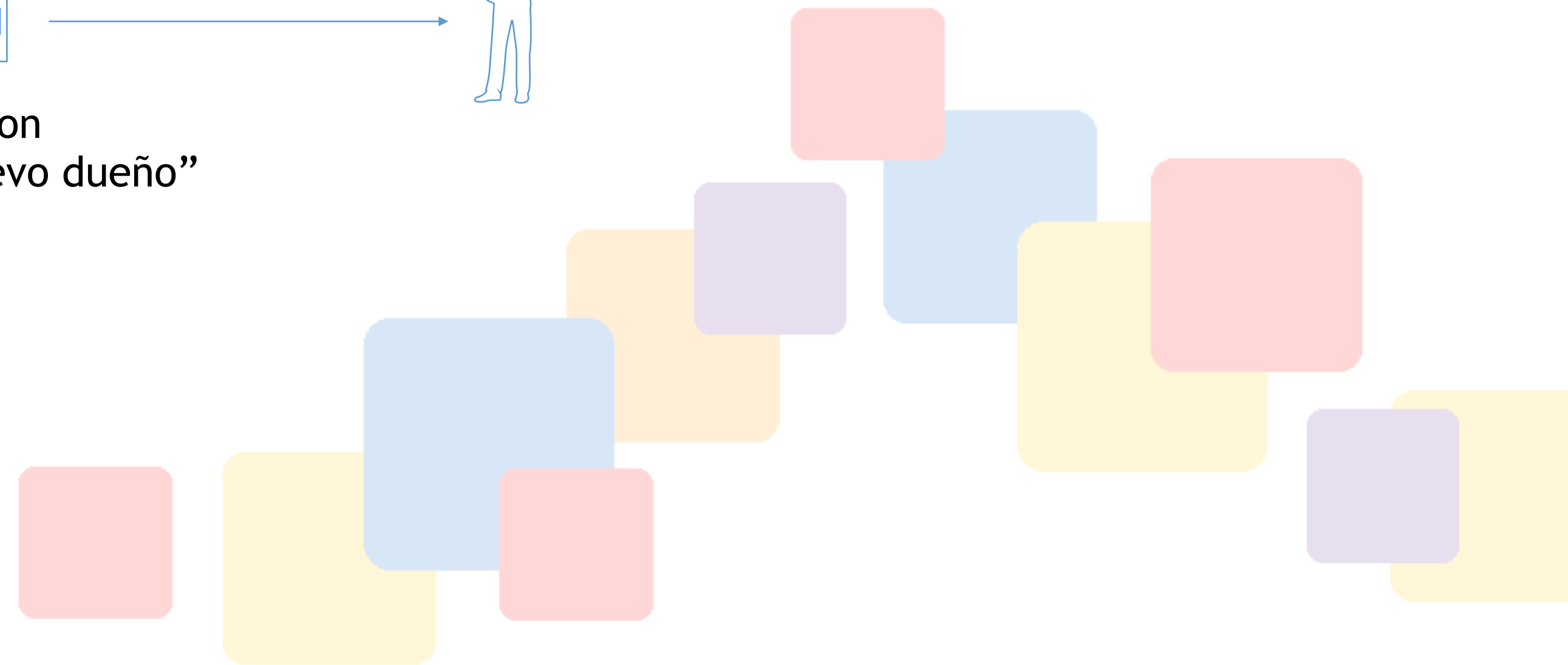
# AZTEC y zk.money

Al transferir



Verificación ZKP

$$\text{val}(A) + \text{val}(B) = \text{val}(C) + \text{val}(D)$$



# Semaphore Protocol

- Permite votaciones secretas
- Revelación de información sabiendo origen pero no fuente exacta





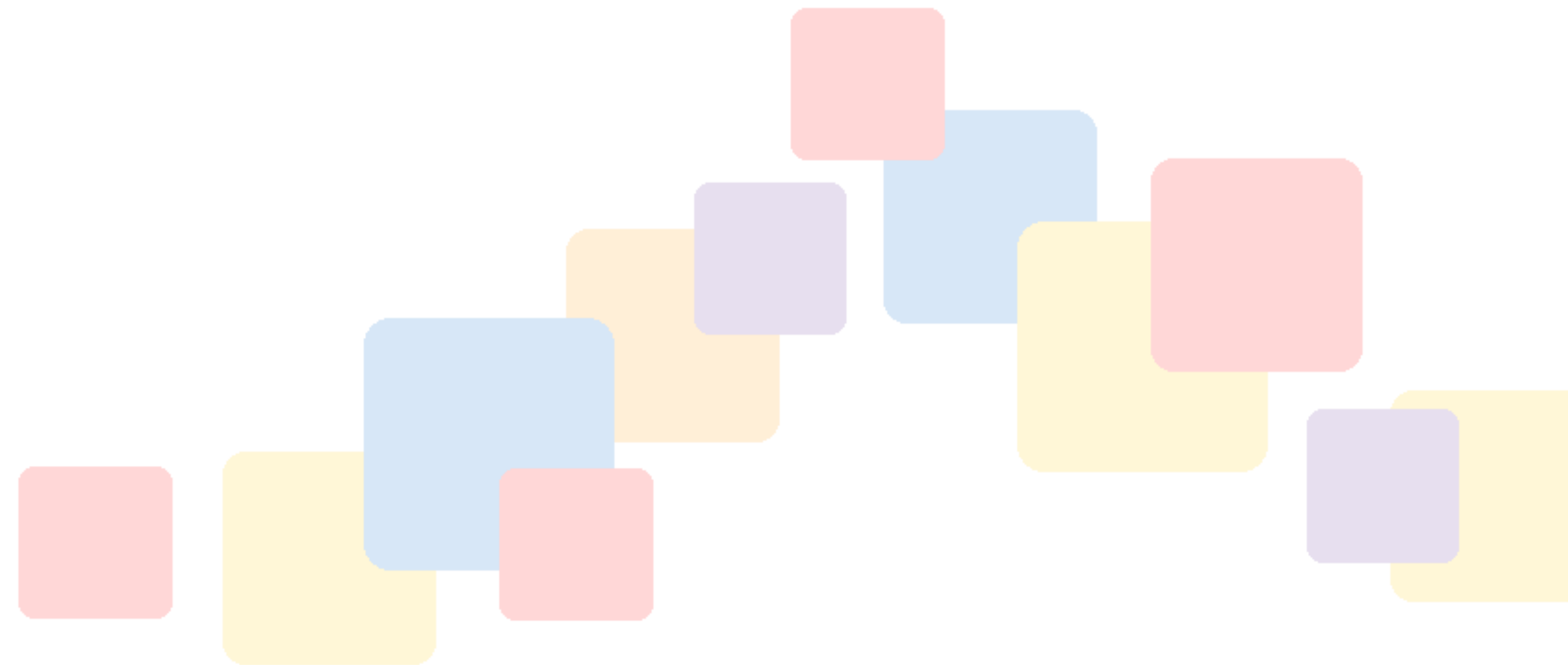
# Semaphore Protocol

- Creo una identidad (par de llaves)
- Me agrego a un determinado grupo
- Puedo escribir un texto y firmarlo
  - Se puede verificar que soy parte del grupo
  - No se puede saber quien soy

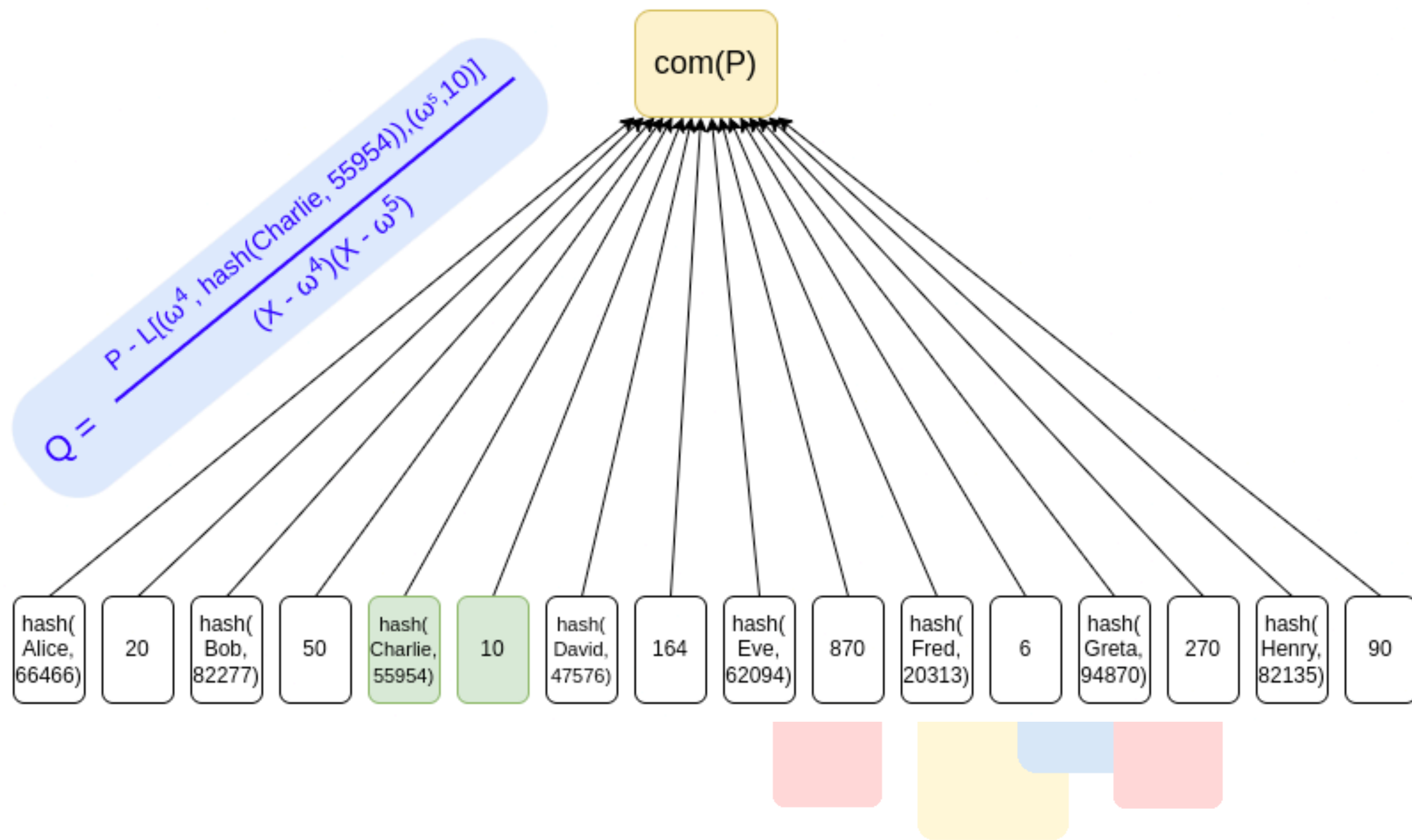


# Proof of Reserves

- Última moda para los exchanges que manejan depósitos de criptos
- Permiten hacer una prueba de que el Exchange tiene las reservas que dice tener



# LS



# Demostración Práctica de Semaphore



# Zk Starks

- Zero knowledge Scalar Transparent Argument of Knowledge
  - Tres principios: Interactive Proofs, Probabilistically Checkable Proofs
  - No necesitan un trusted setup
  - Sólo usan algoritmos hash (en teoría, cuanto resistentes)
  - Generan pruebas mucho más largas



# Nota final sobre privacidad

- En blockchain, los datos van a persistir un muy largo tiempo
- Y van a ser públicos
- Algo que hoy sea privado, quizás no lo sea mañana
  - Vulnerabilidades en algoritmos
  - Mejores GPUs
  - Computadores Cuánticos



# Integración con UX



# Integración con UX

- Hasta ahora todo ha sido
  - Código
  - Remix
  - Algo de Hardhat
- ¿Dónde entra el usuario?





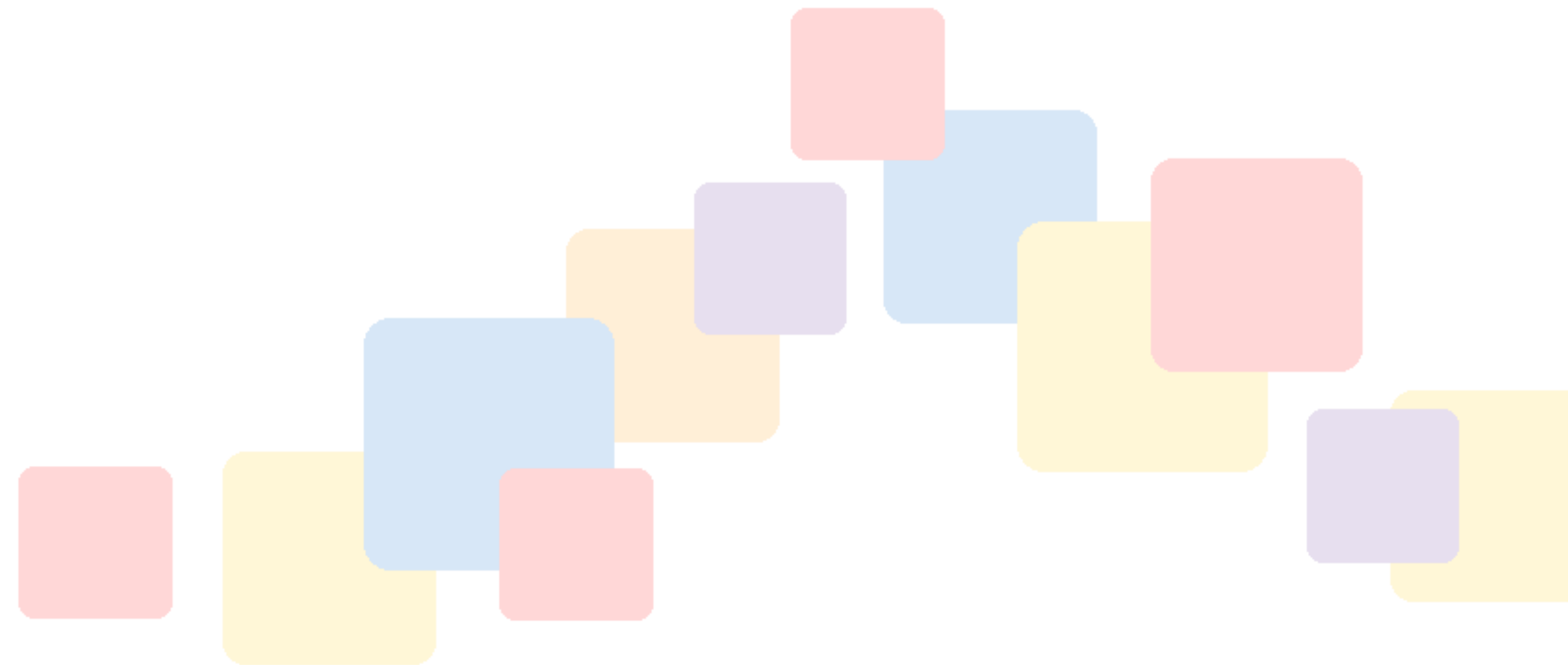
# Todo o casi todo es en Javascript

- Las llaves privadas están en poder del usuario
- La firma de transacciones debe hacerse del lado del cliente
- El lenguaje universal del lado del cliente es Javascript
  - React, Angular, Vue, etc
  - Aplicaciones Mobile



# Nota sobre Mobile

- El ecosistema Apple es altamente hostil al desarrollo cripto
  - No por temas técnicos sino de negocio
  - Tendencia a considerar compras cripto como compras “in app”
- Pago del 30%
  - Valores criptos
  - NFTs
  - Uso del gas
  - Etc



# Librerías de Integración

- Web3.js
  - Clásica
- Ethers.js
  - “Retador”
  - Actualmente con más uso en proyectos nuevos



# Hay algunas similitudes

- Se parte por configurar un provider
  - Metamask, WalletConnect
- Se referencian los contratos inteligentes
  - Address + ABI
- Se generan las transacciones
  - Se pide la firma al usuario



# Ejemplo Práctico



# Principios de Identidad Soberana



# Disclaimer

- Esto es tema en desarrollo
- No hay un consenso sobre como encararlo
- Esto es un resumen de las principales tendencias



# ¿Dónde entra la identidad?

- Hasta ahora, hemos tratado con 0x3e454b....
  - ¿Cómo relacionar eso con Patricio López?
  - ¿Lionel Messi?
  - ¿Copec?





# ¿Qué es la identidad?



- Lionel Messi
- Argentino
- 35 años
- Futbolista
- 7 veces balón de oro
- Campeón Mundial 2022
- 10 veces Campeón de Liga
- 4 Orejonas
- Casado con Antonella Rocuzo
- Padre de 3 hijos
- Condenado por evasión de impuestos
- Mejor Jugador de la Historia



# ¿Qué es la identidad?

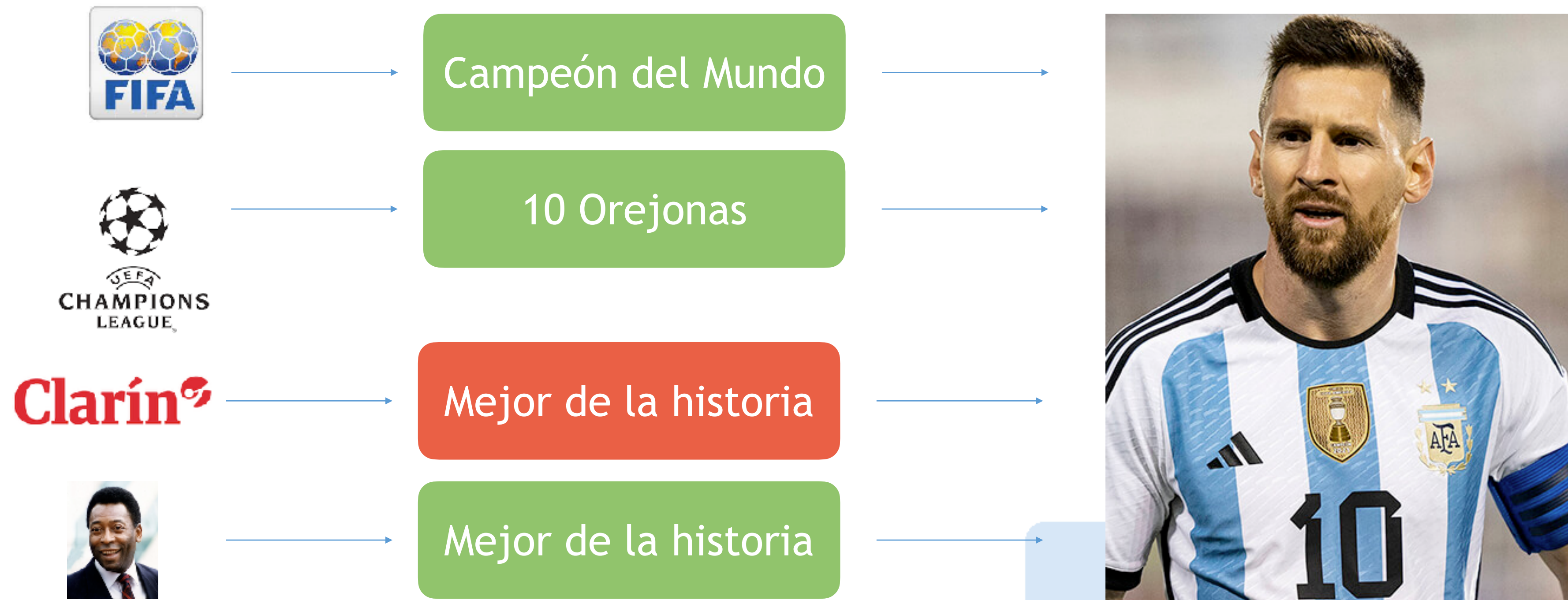


- Patricio López
- Ingeniero Industrial Eléctrico
- Arquitecto Blockchain
- Casado, padre de 1 hija
- Socio de Andes Blockchain
- Hinchas de Universidad Católica
- 46 años

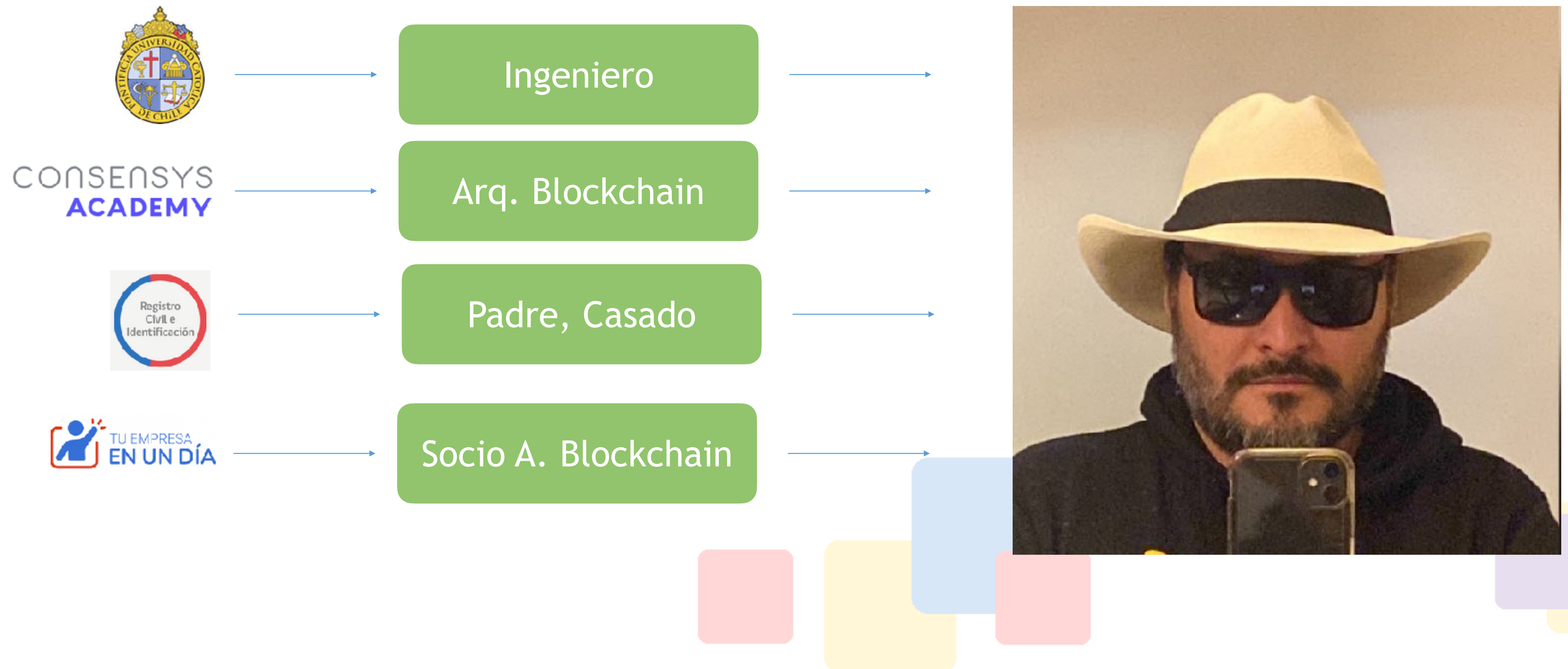




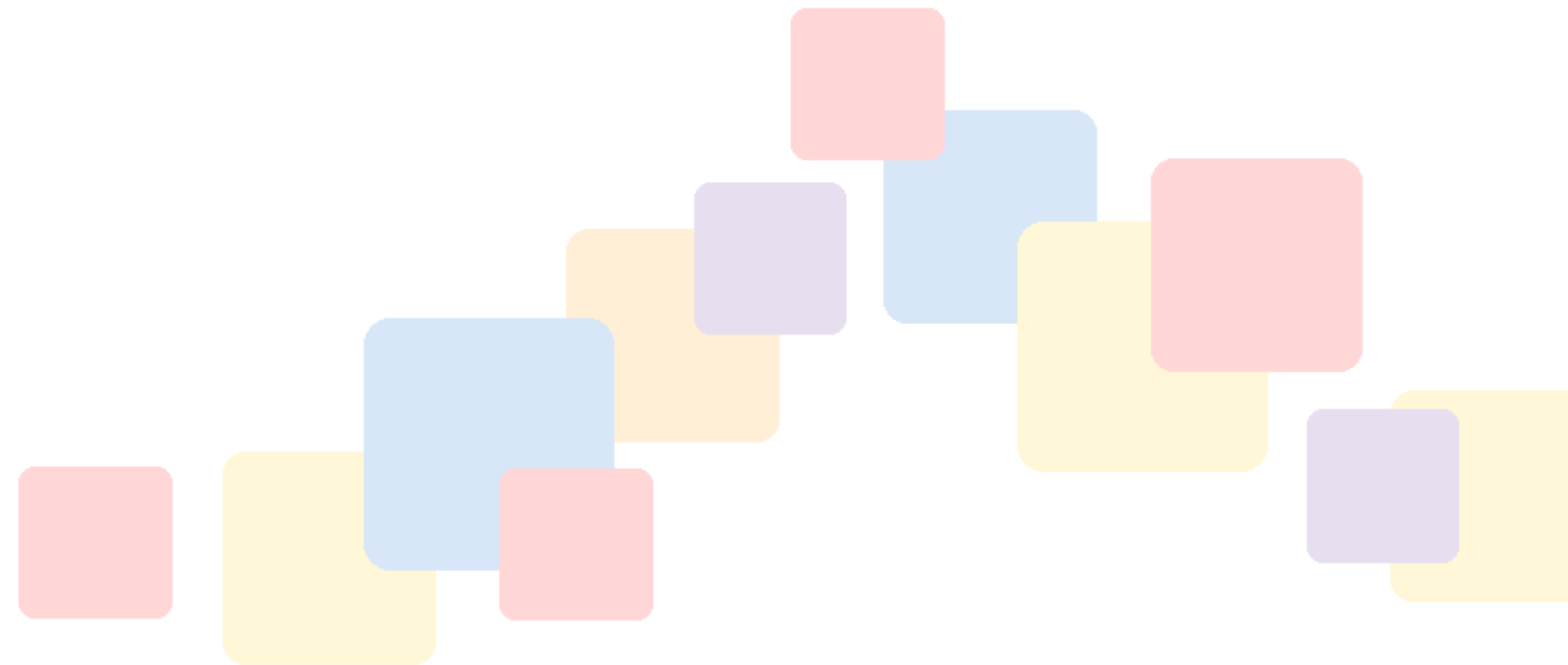
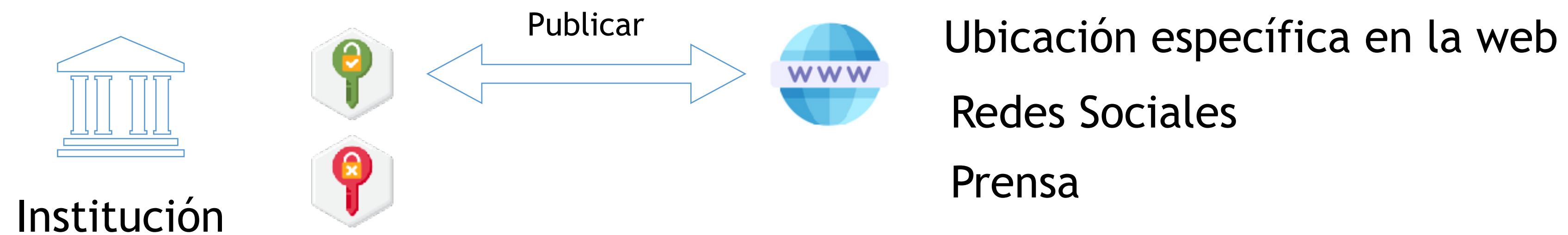
# Patrón: Emisor, Atributo, Destino



# Patrón: Emisor, Atributo, Destino



# El Mecanismo de los Attestation



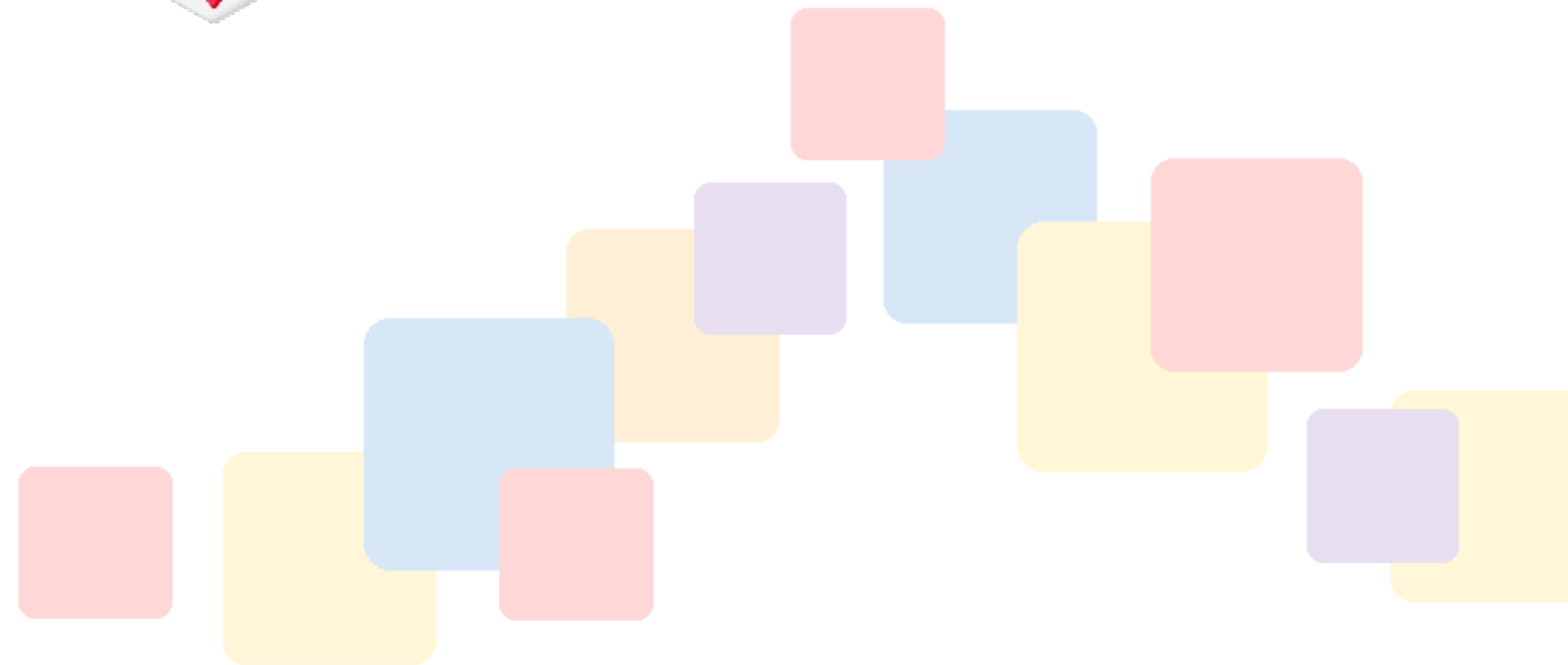
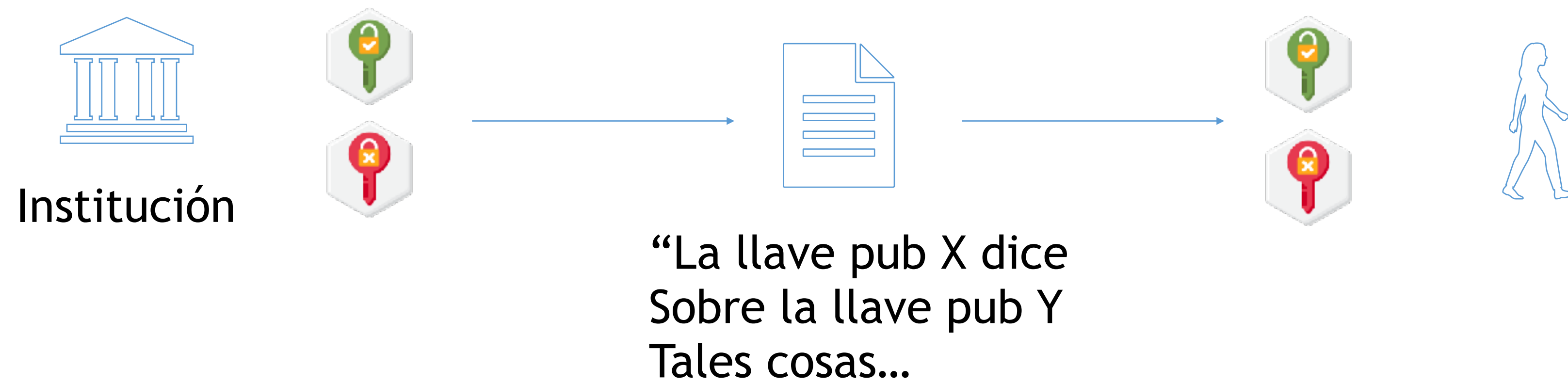
# Componentes de una solución SSI

- DID
- DID Resolver
- VC
- Attester
- Verifier
- Identity Hub



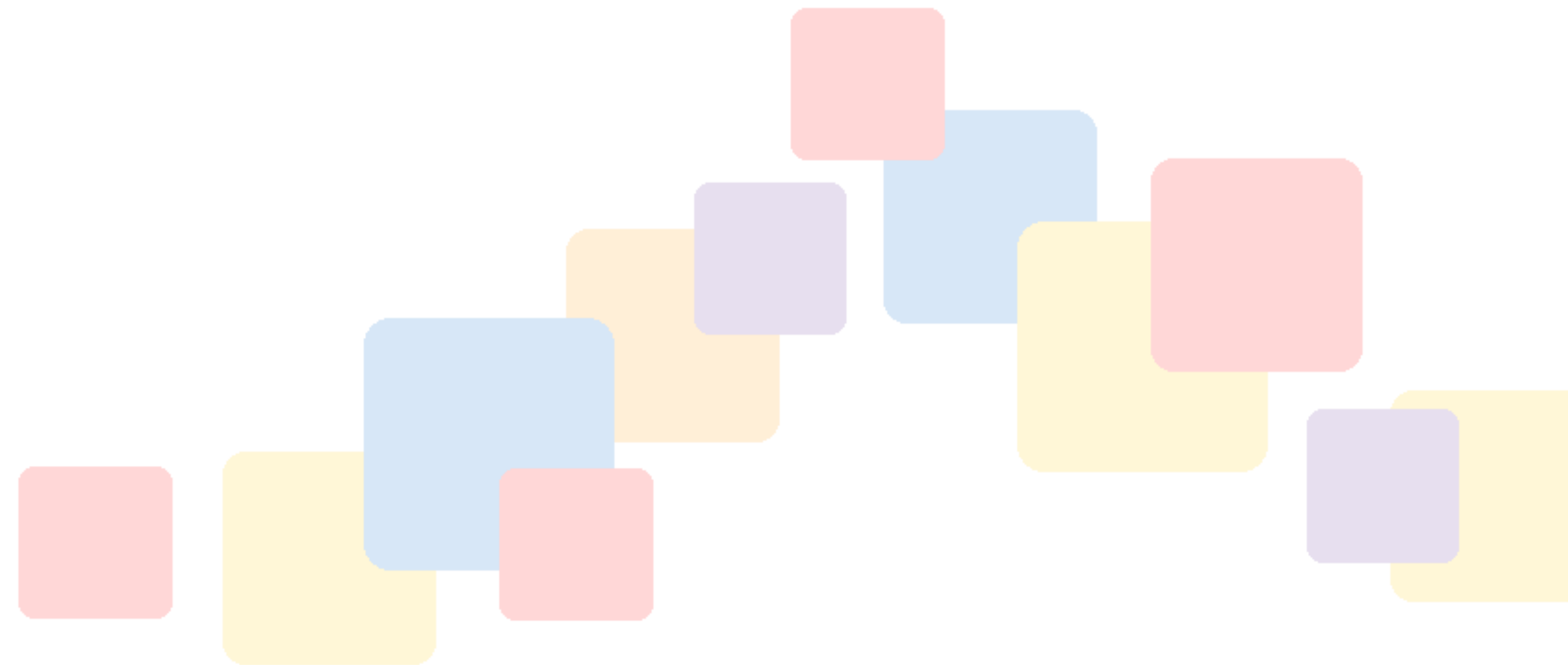


# Attestation



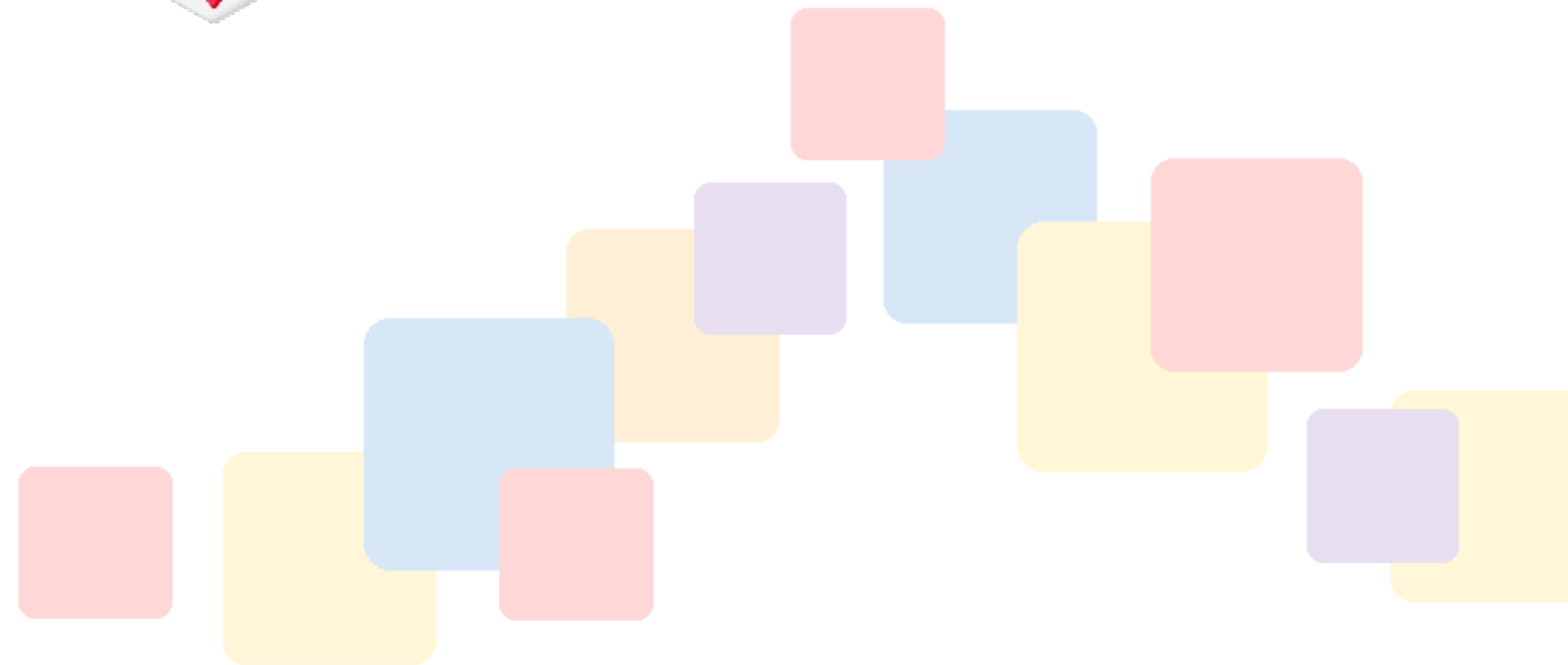
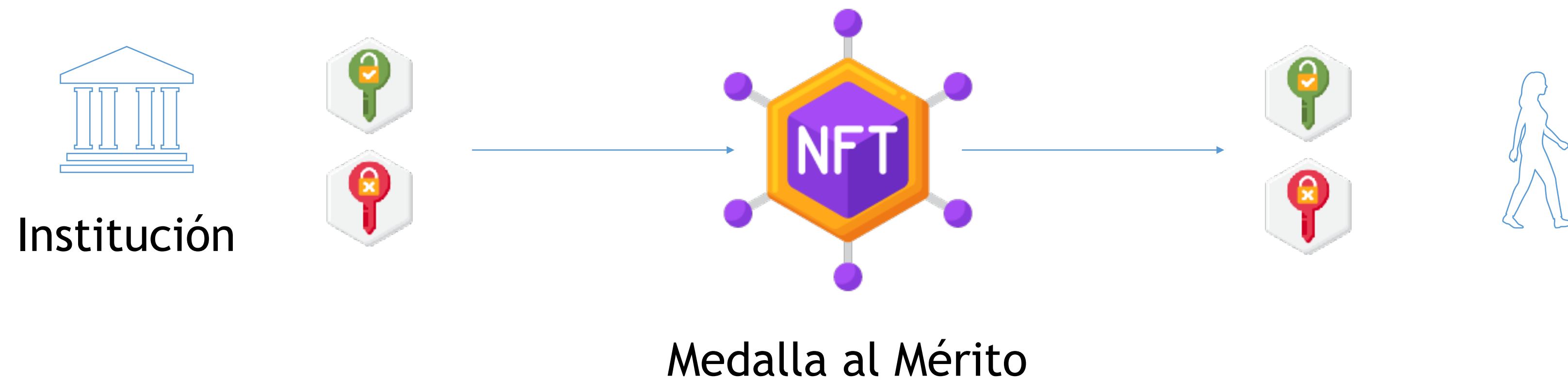
# Algunos principios de diseño

- Minimalismo
- Portabilidad
- Persistencia
- Consentimiento





# Soulbonded NFT



# Proof of Attendance and Participation



La llave X participó  
Del evento Y

