



VI CERTIFICADO DE EXTENSIÓN UNIVERSITARIA EN
TECNOLOGÍAS BLOCKCHAIN



Antonio Tovar · Iván San José



VITALIK BUTERIN

Programador y escritor ruso-canadiense que, con tan solo 19 años, revolucionó la tecnología Blockchain en 2013.

□ La Génesis de Ethereum

Transformó la tecnología Blockchain con Ethereum, al demostrar que esta podía albergar muchos más usos que el mero intercambio de criptomonedas.

- Blockchain ya no es solo un registro contable, sino una computadora mundial descentralizada.
- La infraestructura y evolución de Ethereum se sustenta a través de las **EIP** (*Ethereum Improvement Proposals*), que recogen las especificaciones técnicas del ecosistema. Dentro de estas destacan los **ERC** (*Ethereum Request for Comments*), una categoría específica que permite la interoperabilidad en la red al unificar los criterios para la creación de **Smart Contract**, **tokens (ERC-20)** y **NFTs (ERC-721)**.



CUENTAS TRADICIONALES

En Ethereum, todo comienza con una dirección que puede poseer activos e interactuar con el mundo descentralizado.

❑ El problema: dos cuentas limitadas. Una meta clara.

■ Cuentas de propiedad externa (EOAs):

- ÚNICAS QUE INICIÁN TRANSACCIONES DE FORMA AUTOMÁTICA.
- CONTROLADAS POR CLAVES PRIVADAS Y FIRMAS MANUALES (ECDSA).
- SIN RECUPERACIÓN DE LA CLAVE PRIVADA POR PÉRDIDA O ROBO.
- INCAPACIDAD DE LÓGICA PROGRAMABLE.
- PAGO DE GAS EN TOKEN NATIVO SIN POSIBILIDAD DE DELEGAR A TERCEROS.

■ Contratos inteligentes (Smart Contracts):

- CONTIENEN Y EJECUTAN CÓDIGO, PERMITIENDO USAR LÓGICA PROGRAMABLE.
- DEPENDEN DE LAS TRADICIONALES (EOAs) PARA INICIAR TRANSACCIONES.
- NO PUEDEN PAGAR GAS.



ABSTRACCIÓN DE CUENTAS

EOAS + SMART CONTRACTS = SMART ACCOUNTS

❑ Tu Wallet, tus reglas: La solución definitiva

- La fusión de ambos mundos:
 - CUALQUIER CUENTA FUNCIONA CON LÓGICA PERSONALIZABLE COMO LOS *SMART ACCOUNTS*.
 - INICIA Y PAGA SUS PROPIAS TRANSACCIONES COMO UNA EOA.

YA NO ES NECESARIO QUE EL PROTOCOLO DIGA:
“UNA TRANSACCIÓN ES VÁLIDA SI TIENE UNA FIRMA *ECDSA* CORRECTA”.

AHORA LA VALIDACIÓN SE ABSTRAE Y CADA CUENTA DECIDE SUS PROPIAS REGLAS.

❏ ¿QUÉ OBSTÁCULOS EXISTEN? ¿CÓMO LOS SUPERAMOS?



FIRMA MANUAL Y CONTROL POR CLAVE PRIVADA.



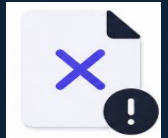
PASSKEY, MULTIFIRMA Y OTROS MÉTODOS DE AUTENTICACIÓN.



SIN RECUPERACIÓN POR PÉRDIDA O ROBO.



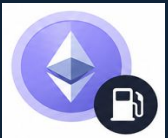
SOCIAL RECOVERY (“GUARDIANES”), RECUPERACIÓN POR HEREDEROS, ETC.



INCAPACIDAD DE LÓGICA PROGRAMABLE.



MÓDULOS DE VALIDACIÓN PERSONALIZADOS, SESSION KEYS, BATCHING, LÍMITES DE GASTO, ETC.



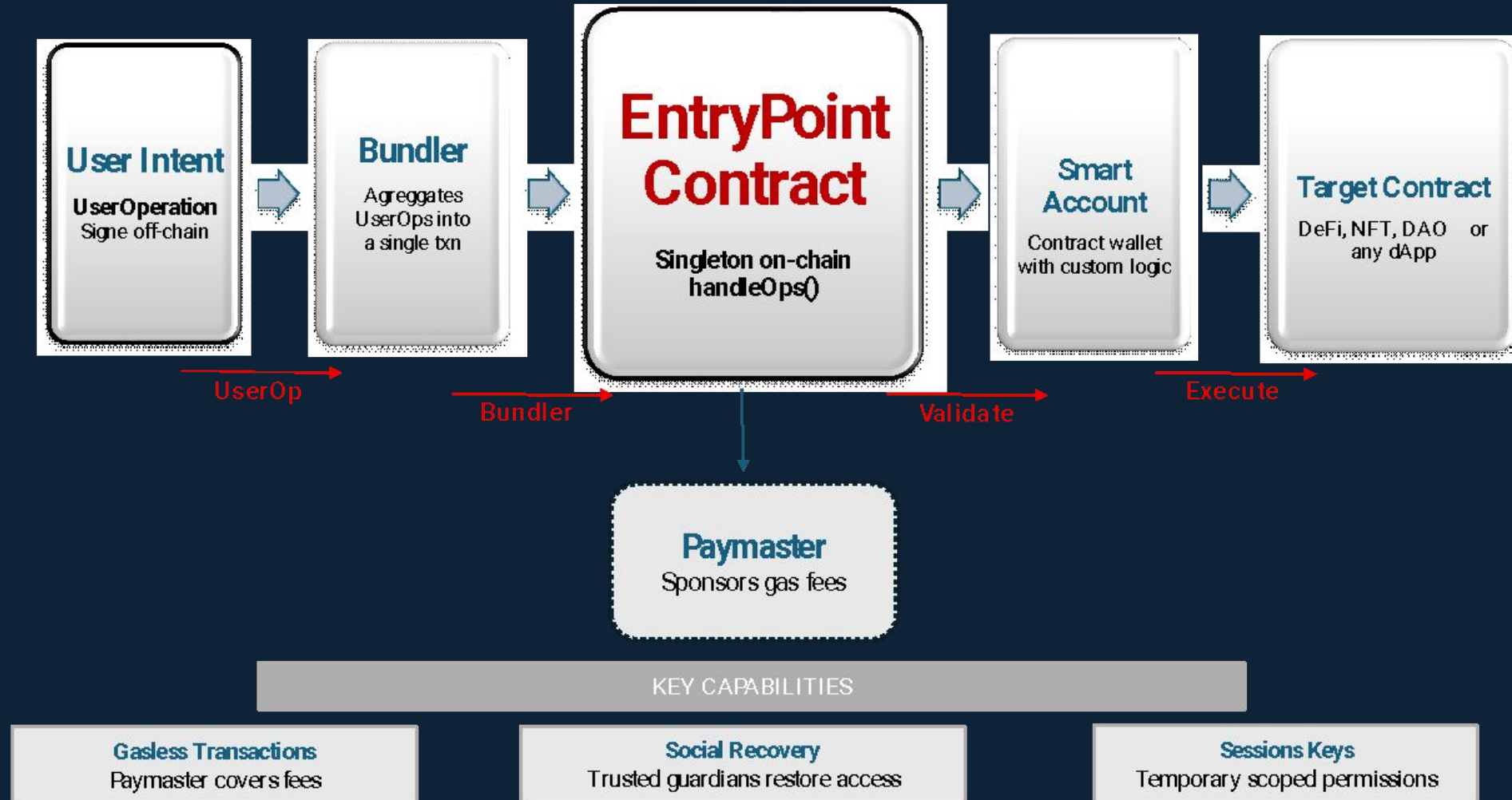
PAGO DE GAS EN TOKEN NATIVO SIN DELEGAR A TERCEROS.

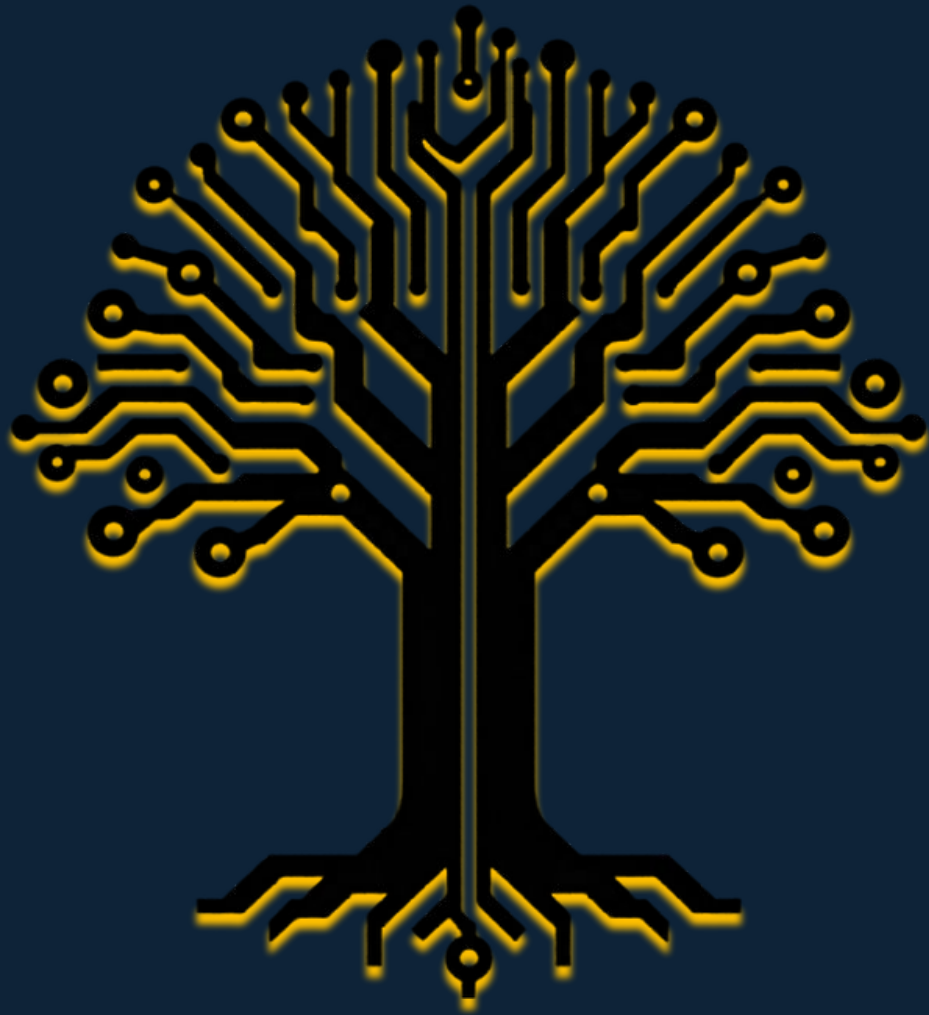


PAYMASTER: PATROCINIO DE TRANSACCIONES O PAGO DEL GAS EN OTROS TOKENS.

ERC – 4337 Account Abstraction

Transaction flow architecture





Hereditary

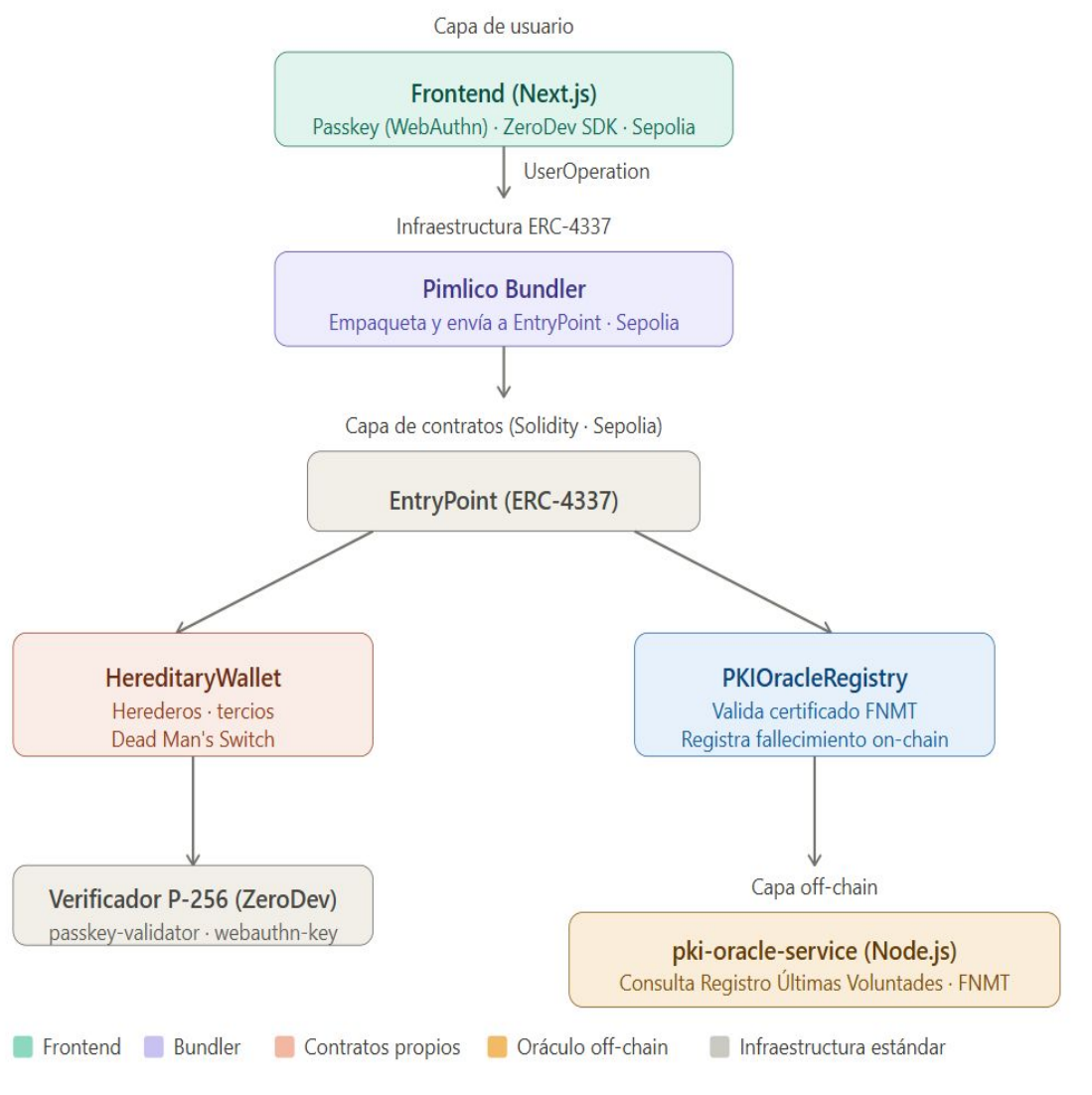
WALLET

Securing Your Digital Legacy

❑ “LA LEGÍTIMA”: Código Civil español (Art. 806+)

Hereditary Wallet es un sistema de herencia digital en Blockchain construido sobre Ethereum Sepolia, que permite al testador configurar y distribuir su herencia de forma segura, respetando la estructura de tercios del Código Civil español.

- **Tercio de legítima estricta:** estrictamente a los herederos forzosos. Se reparte a partes iguales.
- **Tercio de Mejora:** opción de reparto de forma desigual entre los herederos forzosos.
- **Tercio de libre disposición:** No tiene restricciones legales, permite testar a favor de cualquiera (amigos, ONGs, etc.).



FLUJO DE IMPLEMENTACIÓN

ZERO DEV + PIMLICO + SOLIDITY + NETX.JS +
SEPOLIA TESTNET.

CONSTRUYENDO SOBRE ZeroDev



- ❑ **Testador accede con una passkey** (huella o PIN), sin necesidad de contraseñas ni seed phrases.
- ❑ Desde su **Smart Account ERC-4337**, configura la herencia dividida en tres tercios. Los herederos se identifican por un hash de sus datos personales garantizando privacidad on-chain conforme al RGPD.
- ❑ **Dead man's switch**: si el testador no registra actividad en el plazo establecido, cualquiera puede activar la herencia. Un oráculo mock simula el Registro de Últimas Voluntades del Ministerio de Justicia, que certifica el fallecimiento del testador. Una vez activada, cada heredero introduce sus datos y reclama su parte automáticamente.

Gracias

Thanks Folks

VI CERTIFICADO DE EXTENSIÓN UNIVERSITARIA EN TECNOLOGÍAS
BLOCKCHAIN

Isaac Agudo · Rodrigo Román · Antonio Moreno · David Núñez · José Ramírez · **Marco López** ·
Carlos Sánchez · Rubén Ríos · Manuel Montenegro · Daniel Morales · David Arroyo · Ravel Moreno · Carlos Guzmán



Antonio Tovar · Iván San José