



BVCC Agent Wallet

Una wallet no custodial que le pone a un agente de IA límites de gasto que hace cumplir el propio contrato.

Código abierto · ERC-4337 + passkeys · Cinco mainnets · Creada por BlockVenture Chain Capital

BETA PÚBLICA

NO CUSTODIAL

GPL-3.0

SIN KYC

AUTOALOJABLE

EL PROBLEMA

Hoy, para que un agente de IA pueda transaccionar, le das una clave privada. Una clave privada no tiene techo. Si le cuelan un prompt injection, si alucina un destino o si la clave se escapa de un fichero de configuración, todo lo que hubiera en esa wallet se ha ido, y no había nada on-chain en posición de impedirlo.

La respuesta habitual es un servidor en medio que decide qué transacciones se firman. Funciona, y desplaza el problema. Ahora confías en el servidor, y quien lo opere puede firmar lo que le apetezca.

BVCC mete los límites en el contrato. Una clave de agente filtrada vale lo que le quede de presupuesto, no la cuenta entera.

QUÉ ES REALMENTE DISTINTO

Casi todo el trabajo sobre wallets para agentes se queda en el tope de gasto. El problema difícil es que un tope no dice nada sobre la intención. Un agente autorizado a hacer swaps en Uniswap con 500 \$ de presupuesto puede enrutar ese swap para que la salida acabe en la dirección de un atacante, y nunca se pasa de 500 \$.

Así que la wallet inspecciona la llamada. En un swap por el Universal Router de Uniswap fija el argumento del destinatario a tu propia wallet y exige que los bytes de comando coincidan exactamente. Cualquier otra cosa revierte con `PinnedArgMismatch()`. El agente puede operar. No puede operar en beneficio de otro. Detrás hay 34 tests adversariales y 42 del validador.

QUÉ PUEDE HACER DE VERDAD UN AGENTE

Préstamos — Aave v3

19 herramientas

Depositar, pedir prestado, devolver, retirar. Más cuatro planificadores que deshacen una posición viva: desapalancar, cerrar, cambiar el colateral, cambiar la deuda — cada uno respetando un suelo de health factor y abortando si el oráculo se desvía.

Liquidez — Uniswap v3 y v4

14 herramientas

Abrir una posición en el rango que elijas, cobrar comisiones, reducir, cerrar. Incluye pools de ETH nativo en v4, con los hooks controlados por un registro con timelock de 48 h.

Swaps y transferencias

18 herramientas

Uniswap v3 y v4, ETH nativo a la entrada y a la salida, envíos de ERC-20 y nativos, aprobaciones.

Antes de actuar

15 de simulación

Casi toda escritura tiene su dry-run, que devuelve el gas y el motivo del revert, así que un modelo puede comprobar si algo funciona antes de gastar. Y cuatro guías que puede leer.

PRUÉBALO SIN ARRIESGAR NADA

```
$ BVCC_MCP_READONLY=true npx -y @bvcc/agent-mcp
► 27 herramientas registradas · sin ninguna de escritura
► lee saldos · cotiza swaps · simula — no puede mover fondos
```

Quita la variable y el mismo servidor expone las 53. Sirve cualquier cliente MCP: Claude, Cursor, LM Studio, Hermes. Cada llamada sigue teniendo que pasar por el contrato.



EN CIFRAS

312 tests de Foundry unit · fork · fuzz	53 herramientas MCP 12 lectura · 15 sim · 26 escritura	27 en modo solo lectura sin ninguna de escritura
6 redes, una sola dirección determinista con CREATE2	35 bytes de margen EIP-170 24.541 de 24.576	0 bases de datos, emails o KYC la passkey deriva la dirección

SEGURIDAD, ENTERA

Críticos	2	ambos corregidos
Altos	3	1 abierto
Medios	5	3 corregidos
Bajo	1	corregido
Informativos	2	

Revisión interna, cuatro rondas. **Sin auditoría externa.** Nueve hallazgos corregidos en bytecode desplegado y verificado en las seis redes. BVCC-03 sigue abierto: con un allowance previo, fijar el destino de una llamada no acota su valor. Ten cero allowances antes de autorizar a un agente. El informe de 44 páginas está publicado.

LÍMITES QUE HACE CUMPLIR EL CONTRATO

- **Presupuesto** por periodo con renovación automática, más topes diario, por transacción y total
- **Por token**, presupuesto diario y total, guardado por dirección y sobrevive a reautorizar
- **Listas blancas** de tokens, protocolos y destinatarios; los agentes deben ser EOA y nunca pueden llamar a la wallet
- **Políticas de llamada** que fijan argumentos concretos del calldata en las llamadas DeFi
- **Caducidad y pausa inmediata**, en manos del dueño, firmadas con tu passkey
- **Recuperación** por 2 de 3 guardianes con timelock de 48 h; completarla pausa a todos los agentes

PROBADO EN MAINNET

Swap	Swap del agente en Arbitrum por el Universal Router. La comisión salió al 0,15 % exacto, al wei.
Préstamo	Ciclo completo en Aave v3 por el agente: supply → borrow → repay → withdraw. Posición cerrada.
Liquidez	Pool nativo ETH/USDC de Uniswap v4: mint → collect → decrease → burn.
Bloqueado	Un swap redirigido a otra dirección revirtió con <code>PinnedArgMismatch()</code> .

STACK

Acceso	WebAuthn / passkeys, P256
Cuenta	ERC-4337 · batching ERC-7821 · firmas anidadas ERC-7739
Contratos	Solidity 0.8.36, Foundry, OpenZeppelin. Toolchain congelado para CREATE2 determinista
App	Next.js 16, viem, wagmi. Inglés y español
Agentes	Model Context Protocol · @bvcc/agent-sdk, @bvcc/agent-mcp (MIT)
Redes	Ethereum · Arbitrum One · Base · BNB Chain · Polygon · Arbitrum Sepolia

Web bvccwallet.blockventurechaincapital.com **Prensa** contact@blockventurechaincapital.com

Código github.com/blockventurechaincapital-crypto **Demo** youtu.be/dWUTaWBk68A

BlockVenture Chain Capital es una marca y proyecto Web3. No es una empresa constituida, ni un banco, bróker, exchange, custodio o entidad financiera regulada, y no guarda, controla ni recupera fondos de usuarios. BVCC Agent Wallet es software experimental en beta pública. Los contratos pueden tener bugs. Kit de prensa, logos y ficha completa en bvccwallet.blockventurechaincapital.com/press