



BVCC Agent Wallet

A non-custodial wallet that gives an AI agent spending limits the contract itself enforces.

Open source · ERC-4337 + passkeys · Five mainnets · Built by BlockVenture Chain Capital

PUBLIC BETA

NON-CUSTODIAL

GPL-3.0

NO KYC

SELF-HOSTABLE

THE PROBLEM

To let an AI agent transact today, you give it a private key. A private key has no ceiling. If the agent is prompt-injected, hallucinates a destination, or the key leaks out of a config file, everything in that wallet is gone, and nothing on-chain was in a position to stop it.

The usual answer is a server in the middle that decides which transactions to sign. That works, and it moves the problem. Now you trust the server, and whoever runs it can sign whatever it likes.

BVCC puts the limits in the contract instead. A leaked agent key is worth its remaining budget, not the account.

WHAT IS ACTUALLY DIFFERENT

Most work on agent wallets stops at a spending cap. The harder problem is that a cap says nothing about intent. An agent authorized to swap on Uniswap with a \$500 budget can route that swap so the output lands in an attacker's address, and it never goes over \$500.

So the wallet inspects the call. For a swap through Uniswap's Universal Router it pins the recipient argument to your own wallet and matches the command bytes exactly. Anything else reverts with `PinnedArgMismatch()`. The agent can trade. It cannot trade on someone else's behalf. There are 34 adversarial tests and 42 validator tests behind that check.

WHAT AN AGENT CAN ACTUALLY DO

Lending — Aave v3

19 tools

Supply, borrow, repay, withdraw. Plus four planners that unwind a live position: deleverage, close, swap the collateral, swap the debt — each respecting a health-factor floor and aborting on oracle deviation.

Liquidity — Uniswap v3 & v4

14 tools

Open a position at a chosen range, collect fees, reduce, close. v4 native ETH pools included, with hooks gated by a registry on a 48-hour timelock.

Swaps & transfers

18 tools

Uniswap v3 and v4, native ETH in and out, ERC-20 and native sends, approvals.

Before it acts

15 simulate

Most writes have a matching dry-run returning gas and the revert reason, so a model can check whether something works before spending. Four guides it can read first.

TRY IT WITHOUT RISKING ANYTHING

```
$ BVCC_MCP_READONLY=true npx -y @bvcc/agent-mcp
> 27 tools registered · all writes removed
> read balances · quote swaps · simulate — cannot move funds
```

Drop the flag and the same server exposes all 53 tools. Any MCP client works: Claude, Cursor, LM Studio, Hermes. Every call still has to pass the contract.



BY THE NUMBERS

312

Foundry tests
unit · fork · fuzz

53

MCP tools
12 read · 15 sim · 26 write

27

tools in read-only mode
every write removed

6

networks, one address
deterministic via CREATE2

35

bytes of EIP-170 headroom
24,541 of 24,576

0

databases, emails or KYC
the passkey derives the address

SECURITY, IN FULL

Critical	2	both fixed
High	3	1 open
Medium	5	3 fixed
Low	1	fixed
Informational	2	

Internal review, four rounds. **Not externally audited.** Nine findings are fixed in bytecode deployed and verified on all six networks. BVCC-03 stays open: with a standing token allowance, pinning a call's destination does not bound its value. Hold zero allowances before authorizing an agent. Full 44-page report is published.

LIMITS THE CONTRACT ENFORCES

- ▶ **Budget** per period with auto-rollover, plus daily, per-transaction and lifetime caps
- ▶ **Per-token** daily and total budgets, kept by address across re-authorization
- ▶ **Allowlists** for tokens, protocols and recipients; agents must be EOAs and can never call the wallet
- ▶ **Call policies** pinning individual calldata arguments on DeFi calls
- ▶ **Expiry and instant pause**, owner-controlled, signed with your passkey
- ▶ **Recovery** by 2-of-3 guardians on a 48-hour timelock; completing one pauses every agent

PROVEN ON MAINNET

Swap	Agent swap on Arbitrum through the Universal Router. Fee came out at 0.15% to the wei.
Lending	A full Aave v3 cycle by the agent: supply → borrow → repay → withdraw. Position closed.
Liquidity	Uniswap v4 ETH/USDC native pool: mint → collect → decrease → burn.
Blocked	A swap redirected to another address reverted with <code>PinnedArgMismatch()</code> .

STACK

Auth	WebAuthn / passkeys, P256
Account	ERC-4337 · ERC-7821 batching · ERC-7739 nested signatures
Contracts	Solidity 0.8.36, Foundry, OpenZeppelin. Frozen toolchain for deterministic CREATE2
App	Next.js 16, viem, wagmi. English and Spanish
Agents	Model Context Protocol · @bvcc/agent-sdk, @bvcc/agent-mcp (MIT)
Chains	Ethereum · Arbitrum One · Base · BNB Chain · Polygon · Arbitrum Sepolia

Site bvccwallet.blockventurechaincapital.com **Press** contact@blockventurechaincapital.com

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

BlockVenture Chain Capital is a Web3 brand and project. It is not an incorporated company, bank, broker, exchange, custodian, or regulated financial institution, and it does not hold, control or recover user funds. BVCC Agent Wallet is experimental public beta software. Smart contracts may contain bugs. Press kit, logos and full fact sheet at bvccwallet.blockventurechaincapital.com/press