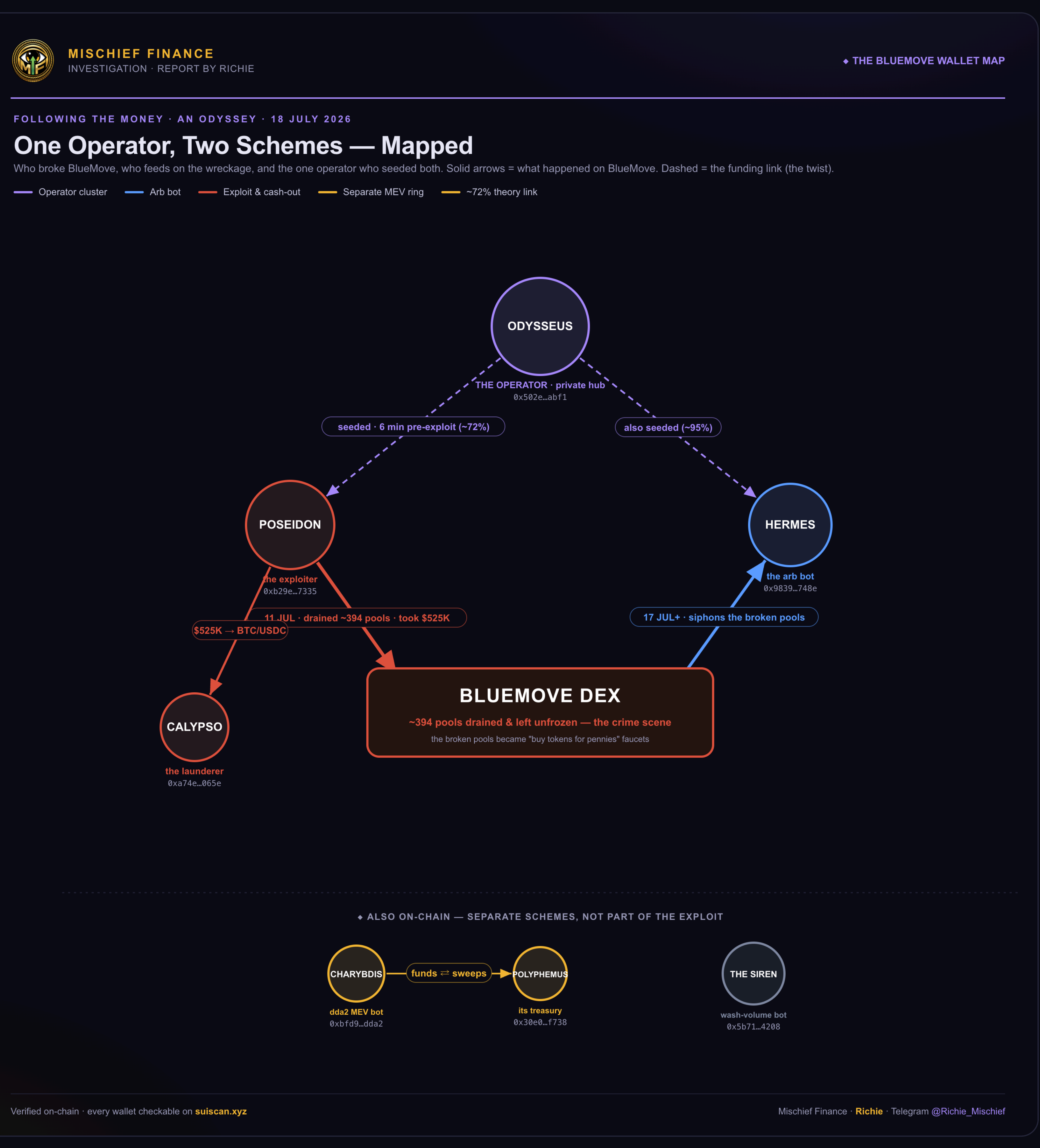
FOLLOWING THE MONEY · A WALLET-GRAPH THEORY · 18 JULY 2026

One Hand Behind the Curtain? Tracing the BlueMove Exploit to Ithaca

This is a **theory piece**, not a verdict. Hard facts are labelled FACT; everything else carries a confidence rating so you can judge it — and rebuild it — yourself. Every wallet is named and linked.

J. W. Waterhouse, *Ulysses and the Sirens* (1891) · public domain. Odysseus, bound to the mast, hears the Sirens' song and lives — the cast below is named for his voyage.

> We traced the BlueMove exploit and the bots feeding on its wreckage through the Sui funding graph. The surprise wasn't the exploit — it was that the wallet **draining the broken pools weeks later** and the wallet that **broke them in the first place** appear to be seeded by the **same private operator.** Here is the whole chain, named, graded, and reproducible.



The wallet map — who broke BlueMove, who feeds on the wreckage, and the operator who seeded both. ↗ **Open the interactive version** (drag the bubbles, zoom, click any wallet to open it on Suiscan).

1 Dramatis Personae

ODYSSEUS PRIVATE HUB · ~90%	A private bot-fleet wallet: 40,000+ txs, arb-style token dust, and only ~25 clean funding recipients. The suspected common source. `0x502e6ef6…965abf1`
POSEIDON FACT	The wallet that executed the 11 July BlueMove exploit — 779 add/remove cycles across ~394 pools. `0xb29e79…6b097335`
CALYPSO FACT	Poseidon's fresh same-day cash-out wallet: ~714,000 SUI (~$525K) → wrapped BTC + USDC → gone. `0xa74ee820…4f75065e`
HERMES FACT	The arbitrage bot draining the broken pools since 17 July — buys tokens for pennies, resells in the same transaction. Now holds 2,377 SUI. `0x98391d8f…da8748e`
AEOLUS FACT	A 4-transaction relay that carried Odysseus's seed straight into Hermes (8-minute pass-through). `0xfa21ca5c…b404fdcc`
SCYLLA FACT	A sub-wallet Odysseus batch-deployed on 25 Apr 2025; it funded Poseidon 6 minutes before the exploit. Later grew into a 460-recipient distributor. `0x50fc775d…e77ae03`
CHARYBDIS (dda2) SEPARATE RING · ~95%	The MEV / flash-swap bot that price trackers mislabelled as the "big seller" dumping SUITRUMP. Real and active — but a net-neutral arb bot, and part of its *own* coordinated ring (with a treasury it sweeps to), not Odysseus's chain. `0xbfd9fa07…6fe3dda2`
THE SIREN FACT	A flash-loan arb bot generating an estimated 9–18% of Sui's entire daily DEX volume on its own — almost all of it wash / flash-loan churn. `0x5b712236…09d94208`

2 The story, act by act

Act I — Poseidon (11 July)

FACT

Poseidon exploited a liquidity-provider bug in BlueMove's AMM, cycling add/remove liquidity across ~394 pools in one night and draining the SUI out of each. This is fully on-chain and independently reported.

Act II — The Cash-out

FACT

Poseidon funnelled ~714,000 SUI (~$525K) into Calypso, a wallet created the same day, which converted it to wrapped BTC + USDC via DeepBook & Cetus and moved it off. Both wallets went dormant that night.

Act III — Hermes (17 July → now)

FACT

BlueMove never froze the drained pools, so each became a "buy the token for pennies" faucet. Hermes began systematically buying near-free tokens from the broken pools and reselling them into live markets — atomically, inside single transactions. It hit 15+ coins (SUITRUMP, PUMPKIN, TOILET, SHOCK, AAA…) and is still running.

Act IV — One hand behind both

THEORY · ~72%

Here is the twist. Trace the seed money and both Poseidon and Hermes lead back to **Odysseus**:

- **Hermes ← Odysseus (~95%).** Odysseus funded Aeolus with 15.84 SUI on 5 Jun 2025; eight minutes later Aeolus forwarded 15.83 SUI to Hermes — the bot's first-ever coins. A clean, single-purpose pass-through.
- **Poseidon ← Odysseus (~75%).** Poseidon's **only** funding was 242 SUI from Scylla at 20:40 on 11 July — **six minutes before its exploit transactions began.** Scylla is itself a wallet Odysseus batch-deployed (3 + 20 SUI) on 25 Apr 2025.
- **The branches touch.** Aeolus and Scylla also directly funded each other — the two "separate" trails are stitched together.

Combine them and the theory is: **the operator who broke the pools is very plausibly the same operator now profiting from draining them.** The soft spot is Scylla — it later became a 460-recipient distributor, so Poseidon is technically 1-of-many payouts. But the bespoke, six-minutes-before-the-exploit timing is operator behaviour, not a routine drip.

3 A separate ring worth naming

Not everything ties to Odysseus. A different, unambiguously coordinated MEV operation runs alongside — **Charybdis** (`0xbfd9fa07…6fe3dda2`) and its **Polyphemus** (`0x30e0784b…d001f738`). Polyphemus funded Charybdis, Charybdis sweeps its profits back to Polyphemus (146 transfers in a single day), and its sub-wallets shuffle tokens between each other — textbook single-operator control (**~95%**). But it runs a different scheme and is **not** the pool-faucet drainer. Treat it as a separate character, not part of Odysseus's chain.

4 A number that reframes the whole board

While measuring the bots, one stood out: **the Siren** `0x5b712236…09d94208` generates **~$2.4M+ of volume a day on its own — roughly 9–18% of Sui's entire ~$26.7M daily DEX volume**, and once you count every swap leg it touches, likely more. It is flash-loan wash volume: borrow, cycle through 2–4 pools, repay in the same transaction. A meaningful slice of Sui's headline "volume" is a handful of bots trading with themselves.

5 Confidence, at a glance

CLAIM	RATING
BlueMove was exploited on 11 July; ~$525K taken and laundered	FACT
Hermes is draining the unfrozen pools atomically, still active	FACT
Odysseus is a private bot-fleet wallet, not an exchange	~90%
Hermes was seeded by Odysseus	~95%
Poseidon was seeded by Odysseus's sub-wallet, 6 min pre-exploit	~85%
Poseidon and Hermes are the same operator	~72%
Charybdis + Polyphemus are one coordinated MEV ring (separate scheme)	~95%

6 How we did this — so you can too

- **Data:** Sui mainnet JSON-RPC only — `suix_queryEvents` (BlueMove swap events), `suix_queryTransactionBlocks` with `{FromAddress}`/`{ToAddress}` + `showBalanceChanges`, plus Noodles (prices/liquidity) and DefiLlama (chain volume). Nothing private.
- **Faucet detection:** flag BlueMove `Swap_Events` where `amount_y_out / amount_x_in > 1,000,000` — tiny SUI in, enormous token out.
- **Atomic-arb test:** in a drain tx, if the token is bought and sold within the same transaction and the wallet's only net gain is SUI, it's a self-contained arb — no downstream "dumper" wallet exists.
- **Private-vs-public test:** count a wallet's *clean SUI funding recipients* (not swap counterparties). ~25 = private operator; hundreds–thousands = exchange/distributor.
- **Birth-funding trace:** a wallet's *first-ever* inflow is its strongest link. We followed each suspect's first funder, hop by hop, to a common source.
- **Method:** five parallel forensic agents, each on one question, cross-checked against each other.

7 What's left — build on this

- **Close Poseidon↔Odysseus gap.** Scylla's distributor growth is the one weak hop. Cluster its 460 recipients — do others behave like Poseidon (single-use, pre-attack funding)? That would harden ~72% toward certainty.
- **Follow Calypso's BTC/USDC exit.** Which bridge/CEX? That's the trail to a real-world identity.
- **Map Odysseus's full fleet.** Its ~25 funding recipients are a suspect list. What else have they touched — other exploits, other chains?
- **Is Charybdis truly separate?** We found no link, but a deeper cross-check between Odysseus's fleet and the ::jk ring is worth doing.
- **Quantify the wash.** Sum every swap leg (not once-per-tx) to state exactly how much of Sui's reported volume is bot self-trading.

If you extend any of this, the addresses above are the entry points. We'll update as the picture sharpens. — Richie, Mischief Finance