Transaction simulation

The Good, the bad & the ugly

Kim Persson

Co-founder & CTO Blowfish.xyz

The BAD: A naive approach to simulation

The BAD: A naive approach to simulation

- Simulating a transaction is easy
  - `eth_call`, `debug_traceCall` and more
- Adversarial environment
  - Malicious or malformed tokens
  - Fake transfer events
  - Red-pill attacks
    - Contracts altering behavior based on global variables like `tx.gasprice`, `block.coinbase` & `block.basefee`[1]
- BAD simulation can do more harm than good

1 https://zengo.com/zengo-uncovers-security-vulnerabilities-in-popular-web3-transaction-simulation-solutions-the-red-pill-attack/

The UGLY: The current state of simulation

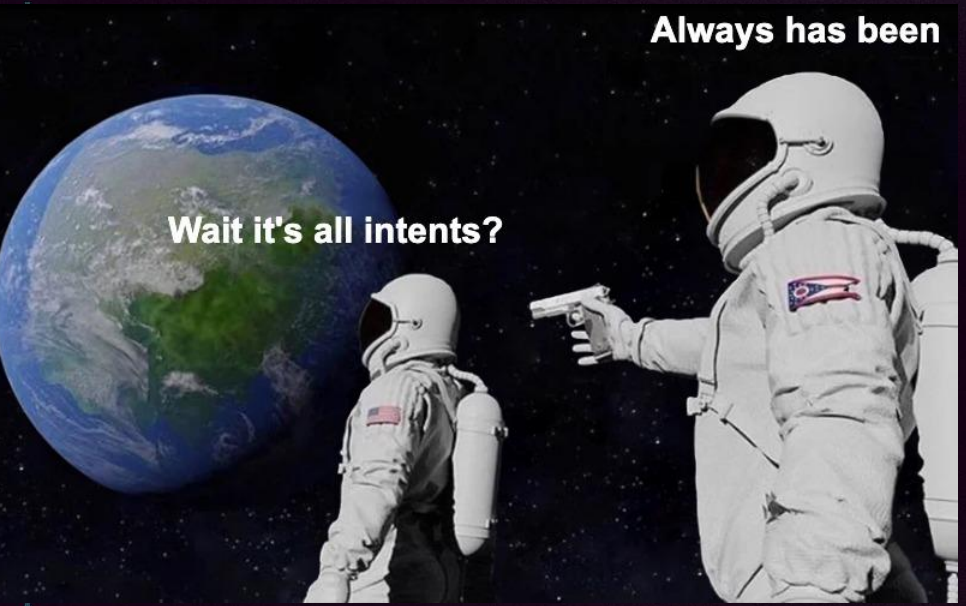
The UGLY: Current state of simulation

- Custom EVM execution environment
  - Mirror on-chain environment as closely as possible
  - Look at changes in state rather instead of events
  - Makes multi chain support difficult
- Does this solve the simulation problem?

The UGLY: Simulation manipulation

- Exploiting simulation with bit-flip attacks
  - One of the common attacks we see on Solana and similar issues apply to EVM
- Use a private mempool?
  - Attack can still succeed with timing heuristics from the dapp UI

- Enforcing simulation results on-chain?
  - If execution deviates significantly from the simulation we revert
  - We have been experimenting with this on Solana
    - Showing great potential in the wild 🔥



Enforcing simulation results on-chain ≈ intents

We start thinking about what the user wants to achieve with the interaction. The transaction input becomes secondary.

The GOOD: Simulate user outcomes

The GOOD: Simulate user outcomes

- Intents may be the future of safe onchain interactions.
- How do we get there?
  - Standardized frameworks for translating intent messages into human readable outcomes
  - This is an opportunity to offer a WYSIWYG experience for the user: *Swap 1 ETH for at least 5000 USDC within 1 hour*
- We could eliminate a significant portion of the scams and loss of funds incidents we see today
  - Today users are signing transactions without a full understanding of the potential consequences

Thank you!

Kim Persson

Your CTO & Co-founder, Blowfish.xyz

kim@blowfish.xyz

@kimpers_