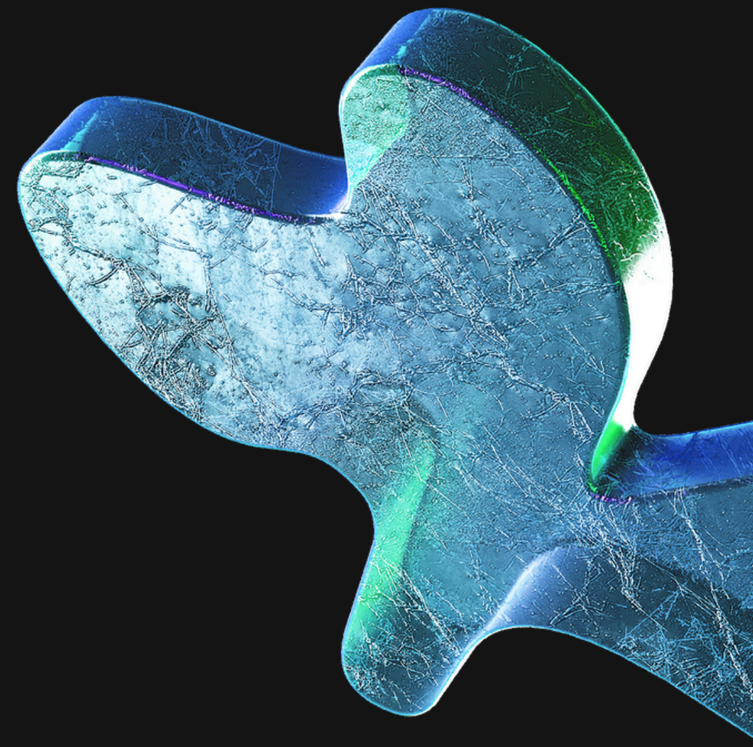

MEV Sentinel: Real-time MEV Bot Detection and Protection Dashboard

Detecting and mitigating front-running, sandwich, and other MEV attacks

techtadka
mateena sadaf
khushi kalinge
nhikhitha m

Problem Statement

- MEV (Maximal Extractable Value) bots exploit DeFi traders and NFT buyers by front-running with higher gas fees.

- Leads to slippage, unfair trades, and financial losses for regular users.

- Need real-time detection and prevention solution.

Project Goals

- Detect suspicious mempool behavior (sandwich attacks, front-running, MEV patterns).
- Visualize flagged transactions, impacted users, and estimated slippage losses in real-time.
- Optionally integrate private transaction relayer to safely submit transactions.
- Bonus: Provide simulation mode for users to test transactions pre-submission for MEV risks.

Technologies Used

Smart Contracts: Solidity with optimizations and secure patterns

Blockchain: Ethereum (or target chain)

Smart Contracts: Solidity with optimizations and secure patterns

Tools: Flashbots relayer (optional), Etherscan API for transaction details

Frontend: React (based on screenshots)

Smart Contract Development and Audit of Telecommunications

- Reviewed and optimized provided Solidity contract to eliminate high-severity vulnerabilities.
- Improved AuditExpress score significantly (mention before/after if available).
- Refactored code for efficiency and security best practices.
- Flattened contract for audit submission.

Key Features - Dashboard Overview

REAL-TIME MEMPOOL MONITORING FOR PENDING TRANSACTIONS AND GAS PRICE.

TOP MEV THREAT DETECTION WITH ESTIMATED EXTRACTION VALUE AND RISK LABELS.

MEV BOTS AND SANDWICH ATTACK ATTEMPTS TRACKED LIVE.

Key Features - Attack Detection

- DETECTION OF FRONT-RUNNING, SANDWICH ATTACKS, FLASH LOANS, AND SLIPPAGE EXPLOITS.
- 24-HOUR ATTACK TYPE DISTRIBUTION GRAPH FOR INSIGHTS INTO ATTACK PATTERNS.
- CLEAR METRICS ON DETECTED ATTACKS AND RISK LEVELS.

Conclusion and Future Work

- Achieved effective real-time MEV attack detection and user protection dashboard.

- Smart contract robustness enhanced through audit and optimization.

- *Future enhancements*:
- Integration of private relayer like Flashbots
- Expanded attack detection types
- Automated mitigation or blocking mechanisms