Investigating Arbitrageurs and Oracle Manipulators in Ethereum

Author
Kevin Tjiam
k.c.tjiam@student.tudelft.nl

Supervisor
Prof. Dr. Kaitai Liang
kaitai.liang@tudelft.nl

TU Delft

1 Background

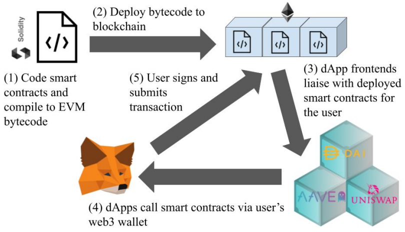


Figure 1: Smart contract lifecycle

- Smart contracts control over **$79B** (USD) of assets on Ethereum [2]
- DeFi: the future of finance™
  - Decentralised
  - Transparent
  - Trustless
- Hundreds of millions of dollars exploited via smart contract vulnerabilities
- Up-to-date knowledge of vulnerabilities and countermeasures must be available

2 Methodology

1. Find prominent attack vectors
2. Buidl test cases of exploits
3. Implement known countermeasures
4. Try to find better countermeasures
5. Evaluate and compare different exploits

3 Vulnerabilities

Transaction-Ordering Dependence

❌ Loss of funds ❌ Consensus-layer instability

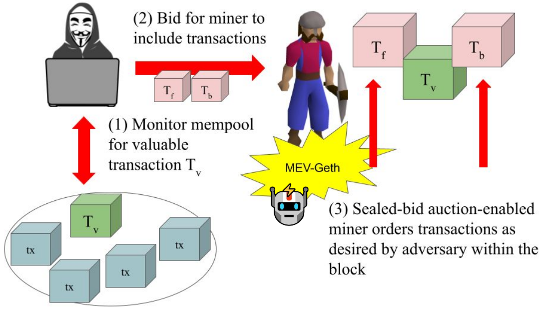


Figure 2: Adversary exploiting TOD vulnerability via Flashbots to extract value from txes

Oracle Manipulation

❌ Loss of funds

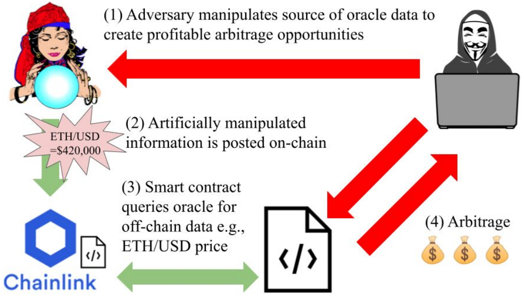


Figure 3: Adversary exploiting a vulnerable price oracle to arbitrage

4 Countermeasures

1. Bypass mempool (Archerswap/Flashbots)
   ✅ Private transactions
2. Order batching (CowSwap)
   ✅ Minimised slippage
3. Commit-reveal on rollups
   ✅ Guaranteed tx ordering

🧑‍💻 Design paradigm: **off-chain computation** [3]

❌ Decreased trust guarantees
❌ Signing raw transactions

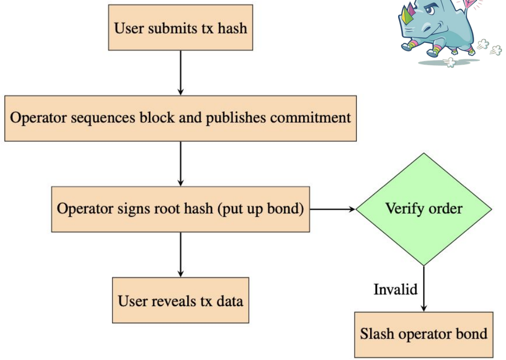
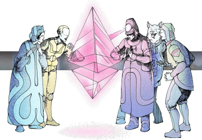


Figure 4: Commit-reveal scheme flowchart



1. Functional audits
   ✅ Expert peer review
2. Time-weighted Average Price (TWAP)
   ✅ Resistant to flash loan + arb attacks
3. M-of-N oracle selection
   ✅ Delegate to trusted entities

🧑‍💻 Design paradigm: **best practices** [3]

❌ Requires human competence and diligence

5 Conclusion

- Many categories of smart contract vulnerabilities [4]
- Highest risks: transaction-ordering (MEV) and oracle manipulation (flash loan attacks)
- Future work: improve trade-offs in trustlessness and decentralisation

Experiments available at:
https://github.com/kevincharm/arbitrageurs-and-oracle-manipulators

References

[1] V Buterin. A Next Generation Smart Contract & Decentralized Application Platform. 2009.
[2] DeFi Pulse: The DeFi Leaderboard: Stats, Charts, and Guides. URL: https://defipulse.com
[3] Bin Hu et al. "A comprehensive survey on smartcontract construction and execution: paradigms,tools, and systems". In: Patterns2.2 (2021),p. 10017.
[4] Zulfiqar Ali Khan and Akbar Siami Namin. "A Survey on Vulnerabilities of Ethereum Smart Contracts". In: arXiv preprint arXiv:2012.14481 (2020).
[5] Michael Rodler et al. "Sereum: Protecting existing smart contracts against re-entrancy attacks". In: arXiv preprint arXiv:1812.05934 (2018).

ethereum.org hero artist: Liam Cobb
Ether (ETH) artist: Viktor Hachmang
DeFi artist: Patrick Atkins