CSci 8271
Security and Privacy in Computing
Day 16: Ethereum frontrunning

Stephen McCamant
University of Minnesota

Frontrunning in general

- Frontrunnnig uses advanced knowledge about a transaction to profit from it
- Previous examples: stock market, domain name registration
- In the stock market, controlled by regulation and law enforcement

Frontrunning types in Ethereum

- Displacement: attack transaction processed before victim
- Insertion: attack transactions sandwich a victim transaction
  - Common with token exchanges
- Suppression: attack transactions postpone a victim transaction
  - Common with timed lotteries

Scalable measurement approaches

- Displacement: look for matching inputs across a sliding window with a Bloom filter
- Insertion: look for triples of exchange transactions within a single block
- Suppression: look for gas exhaustion strategies (e.g., infinite loop)

History and distribution of attacks

- Suppression dominant in 2018, switch to others by 2020
- Insertion attacks follow DEX development
- Suppression is high-risk, high-reward
- Total attacker profit about 18M USD

Implications and mitigations

- Frontrunning generates extra transaction fee revenue for miners (300K USD in this time period)
  - But costs in gas price volatility, congestion
- Fixes/workarounds:
  - Slippage tolerance: present at Uniswap, incomplete
  - Alternative mining architectures: suffer from centralization, miner requirements
  - Submarine commitments: more complex 3-step transactions