Frontrunning

No Author Given

Concordia University

Abstract.

1 Introductory Remarks

1.1 What is frontrunning?

1.2 Miners and their power

2 Related Work

3 Comparison Framework

Solutions:
Criteria:

4 Frontrunning Attacks

4.1 Financial Markets

4.2 Non-financial Applications

Applications, Ghazal, register domains before the user, (domain squatting?)
Other applications (look at Dapps or other blockchain use cases)
Arbitrage (buy before the order, sell to the original order) (other scenarios)
Maker griefing (attack on the system?s reputation itself)
Etherdelta case: Fill the order when cancelling transaction is sent. What would be the profitable scenario here?

5 Implications

Historical evidence of such attacks:
Status ICO [link]
Bancor frontrunning [link, link]
? New attacks:
Ghazal
Find more applications to frontrun, not necessarily monetary gain/financial

6 Mitigations

Commit / reveal methods

- Send the hash first, send the actual data after (sealed-bid auctions)
- Proof of burn methods (generate random addresses with no private keys)

Submarines

- The method described in HD can be optimized and more functional with the new changes to ethereum and solidity
- Submarines 2.0: There can be a new way of doing this (new WRT hackingditributed article), can predict smart contract addresses using the nonce and data of the contract (forwarder/refunder), so funds can be sent to these addresses and then contracts can be deployed
  - Pros: new addresses, no indication of the order (Anonymity-set)
  - Cons: DDoS? Requires 3 transactions for each order? ¿¿ 1 send the funds 2 Deploy the contract 3 call the function
- Other methods? Consensus protocol based solutions?

7 Concluding Remarks