MEV NFT (a ERC-721 fork)

A talk about NFT Arbitrage

Franz Krekeler
University of Hamburg
@filmfranz
What started this talk?

@bertcmiller
@bertcmiller

New MEV just dropped: @moonbirds_xyz arbitrage

Searcher bought for 44 ETH and sold it for 240 ETH in the same transaction, pocketing a cool ~180 ETH for themselves after fees

etherscan.io/tx/0x0659a203b...
Section 1

ELI5: MEV
Question: What happens if you click swap?
Technical explanation

Traditional Markets
Order Sequence's Economic Value is Preserved

Order Matching Servers
Market Gateway Servers

Txn 1
0.3ms
Txn 2
0.7ms
1.2ms
Txn 3

Txn Sequence
1. Txn 1
2. Txn 2
3. Txn 3

Crypto Markets
Order Sequence Determined by Gas Fee, Creating MEV

Public Mempool

PGA

Miner

Block T

Txn Sequence
Txn 2
Txn 3
Txn 1

Block T+1

~ 15s

Block T+2

~ 15s

Source: MEV - A Deep Dive, Part 1 - Liam Zhang & Lau Bao Jie
Proof of Stake
Example before blockchain: Tulip auctions

- Public tulip auctions since 17th-century
- For each flower the clock counts from high price to low price
- Bid by pressing a button

- MEV: 60% of flowers are sold in advance by contract now, bypassing the clocks entirely.

Dutch auction clock (Source: BBC)
Section 1

ELI5: NFT
NFTs

- Smart contract (ERC-721)
- Similar to a token (ERC-20), but non-fungible (entities with ID)
- Top 10 gas spender (OpenSea)
- Search volume:
  - “create erc20 token”: 1K – 10K
  - “create nft”: 10K – 100K
- Conclusion: NFTs are mainstream
Question: What happens if you place a collection bid?
NFT Arbitrage?
Arbitrage is the simultaneous purchase and sale of the same asset in different markets in order to profit from tiny differences in the asset's listed price. It exploits short-lived variations in the price of identical or similar financial instruments in different markets or in different forms.

Definition: Investopedia
Graphic: @jayveg
New MEV just dropped: @moonbirds_xyz arbitrage

Searcher bought for 44 ETH and sold it for 240 ETH in the same transaction, pocketing a cool ~180 ETH for themselves after fees

etherscan.io/tx/0x0659a203b...

Amber Group
@ambergroup.io

Reproducing the $APE Airdrop Flash Loan Arbitrage/Exploit

On March 17th 2022, an airdrop equivalent to 15% of the total supply of ApeCoin was distributed to BAYC/MAYC owners [1]. To claim the...

medium.com

10:46 nachm. · 21. März 2022 · Twitter Web App

13 Retweets  2 Zitierte Tweets  35 „Gefällt mir“-Angaben
WAT DO?

MEV NFT
Step 1: Illuminate the dark forest

- Washtrading: Volume vs. floor price
- Flashbots for frontrunning protection / gas minimization
- Understand bribed mints
- Commit reveal auctions
- Whitelisting

https://mev.tools
Lifecycle of a NFT

Mint
- Can lead to gas wars

Hold
- Holding time indicates if NFT is flipped

Transfer
- Transferred directly or sold using On-Chain / Off-Chain auctions
Step 2
ERC-721 Fork

Code / Idea:
- Store each transfer of an tokenId into a mapping
- Store last block
- Check if token has been transferred in this block
- Revert

contract NonAtomicNFT is ERC721, AccessControl {
    using Counters for Counters.Counter;

    mapping(uint => uint) public tokenBlocks; // tokenId => block number

    bytes32 public constant MINTER_ROLE = keccak256("MINTER_ROLE");
    Counters.Counter private _tokenIdCounter;

    constructor(string memory name, string memory symbol) ERC721(name, symbol) {
        _setupRole(DEFAULT_ADMIN_ROLE, msg.sender);
        _setupRole(MINTER_ROLE, msg.sender);
    }

    /// @notice disallow transfers of a token in the same block
    modifier nonAtomic(uint tokenId) {
        require(tokenBlocks(tokenId) != block.number, "can't transfer in the same block");
        tokenBlocks(tokenId) = block.number;
        _;
    }

    /// @notice disallow transfers of a token in the same block
    function transferFrom(
        address from,
        address to,
        uint256 tokenId
    ) public nonAtomic(tokenId) override(ERC721) {
        super.transferFrom(from, to, tokenId);
    }
}
Conclusion

- Different stakeholders (markets, traders, users)
- NFT long tail
- Didn’t read just ape
- Varying volume
- Users long term interest
- Regulations
Sources

MEV, what do next? - Phil Dahan (Flashbots)
https://www.youtube.com/watch?v=xQydAHiKxuw

This clock was famous, but the internet ruined it.
https://www.youtube.com/watch?v=dAdmzyKagw

Tweet: MEV in dutch auctions:
https://twitter.com/thegostep/status/154154747782079617

MEV - A Deep Dive, Part 1:
https://medium.com/@liamzhang/mev-a-deep-dive-part-1-3f389ef15d32

MEV and Proof-of-Stake
https://www.blocknative.com/blog/mev-proof-of-stake

Tweet: Block Builder MEV
https://twitter.com/The_Babylonians/status/156722775868858777

Gas Spenders
https://dune.com/hildobby/Gas

Images:
https://mev.tools/mev/discipline/2022/08/13/sandwich-connoisseur.html
https://www.history.com/topics/world-war-ii/atomic-bomb-history

Special thanks too:
Alan from Lens Protocol, Bert Miller from Flashbots, Peter, Daniil, JayVeq
Thank you!

Franz Krekeler
f@think-complete.com

@filmfranz
Atomic transactions?

Transaction (tx in the block)

- Method call
- Stack trace
- Revert or execute

# Account balances:

<table>
<thead>
<tr>
<th>Address</th>
<th>Token</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>[receiver] 0x0000000003b322af3eaeleac044bceee416b40</td>
<td>WETH eRSOL</td>
<td>-0.7137 157,629.8664</td>
</tr>
<tr>
<td>UNI-V2</td>
<td>WETH</td>
<td>0.7137</td>
</tr>
<tr>
<td></td>
<td>eRSOL</td>
<td>-157,629.8664</td>
</tr>
</tbody>
</table>
MEV in POS Ethereum

Source: The Babylonians
Forms of MEV

- Insertion
- Ordering
- Blocking
- Sandwiching
- Frontrunning
- Arbitrage