Exploring Auction Mechanisms in Protocol Design

Terence

Offchain Labs

Goals of this talk

Compare and contrast different in-protocol auctions

- High-level overview of the what, how, and why
- Make specific implications to the protocol for each auction
- We will look at:
  - L1: [MEV-Boost], [EIP-7732 block, slot] auctions, [EA, ET] auctions
  - L2: [FCFS], [Priority gas], and [timeboost] auctions

	What is exchanged & **Who** facilitated	**Who** captures profit?	**When** auction concludes vs. reveals?	**Additional notes**
MEV-Boost	Bid(contains block hash) enforced by MEV-Boost **relays**	Builders pay proposers via EL tx, and relays audit bids	Commit and reveal just in time, within 4s to stay safe	It works today with **out-of-protocol** trust but doesn't scale due to timing issues, creating **frictions** with future updates (PeerDAS, FOCIL)
EIP-7732 block auction	Bid(contains block hash) enforced by the **protocol**	Builders pay proposers through the protocol, and assumes honest majority	Commit to block content just in time, and reveal at the half slot (blobs can be revealed earlier)	New FC rules w/ PeerDAS & FOCIL. Reduce out-of-protocol trust. Pipeline consensus & execution. More time to propagate & verify execution payload and blobs. Enables further auction design. May have DA & free optionproblem. Longer tx time inclusion
EIP-7732 slot auction	Bid(contains builder ID) enforced by the **protocol**	Same as block auction	Commit to the right to propose just in time, and reveal at half slot	Similar to block auctions. Local builders face forecasting disadvantage. There's a trusted advantages encourage the use of relays. Less tx time inclusion

	What is exchanged & **Who** facilitated	**Who** captures profit?	**When** auction concludes vs. reveals?	Additional notes
Execution Auction (EA)	Same as 7732 Slot auction but **further ahead in time**	Same as 7732	Auction concludes just in time, with reveal set for a **distant future**	**Reduces timing games**, raises open questions on handling proposer equivocations, and introduces unknown spec complexity
Execution Ticket (ET)	A ticket with a chance to propose a block in the future	**Protocol** captures the profit	Ticket can be purchased anytime, but the lottery occurs in the future	Opens up **MEV-burn**, introduces unknown spec complexity (ex: fee market design), and raises concerns about **multi-slot MEV**

	What is exchanged & **Who** facilitated	**Who** captures profit?	**When** auction concludes vs. reveals?	Additional notes
L2 FCFS (**centralized** sequencer)	User's transaction inclusion via sequencer	Company that operates sequencer or DAO	Just in time. Can have fast confirmation	The sequencer is **trusted**. **Private** mempool. Latency racing. Straightforward to reason about. Transactions can be emitted as a continuous stream
L2 PGA (centralized sequencer)	FCFS + Top of block inclusion	Same as FCFS. Priority fee as additional rev	Per block	Same property as above. Transactions are emitted as blocks
L2 Timeboost (centralized sequencer + **auctioneer**)	FSFS + latency advantage for fast lane holder	Same as FCFS. Bids as additional rev	Per round	Only fast lane holder per round. Reserve bid to prevent collusion. Re-selling and secondary markets are encouraged

Engineers 🤝 mechanism designers 🤝 game theorists 🤝 economists 🤝 and many more

Thank you!

Terence

Offchain Labs

@terencechain