Lissy: Experimenting with on-chain order books

Mahsa Moosavi and Jeremy Clark

Concordia University, Montreal, Canada
seyedehmahsa.moosavi@concordia.ca

Abstract. Financial regulators have long-standing concerns about fully decentralized exchanges that run 'on-chain' without any obvious regulatory hooks. The popularity of Uniswap, an automated market makers (AMM), made these concerns a reality. AMMs implement a lightweight dealer-based trading system, but they are unlike anything on Wall Street, require fees intrinsically, and are susceptible to front-running attacks. This leaves the following research questions we address in this paper: (1) are conventional (*i.e.,* order books), secure (*i.e.,* resistant to front-running and price manipulation) and fully decentralized exchanges feasible on a public blockchain like Ethereum, (2) what is the performance profile, and (3) how much do Layer 2 techniques (*e.g.,* Arbitrum) increase performance? To answer these questions, we implement, benchmark, and experiment with an Ethereum-based call market exchange called Lissy. We confirm the functionality is too heavy for Ethereum today (you cannot expect to exceed a few hundred trade executions per block) but show it scales dramatically (99.88% gas cost reduction) on Arbitrum.

1 Introductory Remarks

There are three main approaches to arranging a trade [19]. In a *quote-driven* market, a dealer uses its own inventory to offer a price for buying or selling an asset. In a *brokered exchange*, a broker finds a buyer and seller. In an *order-driven* market, offers to buy (*bids*) and sell (*offers*/*asks*) from many traders are placed as orders in an order book. Order-driven markets can be *continuous*, with buyers/sellers at any time adding orders to the order book (*makers*) or executing against an existing order (*takers*); or they can be *called*, where all traders submit orders within a window of time and orders are matched in a batch (like an auction).

Conventional financial markets (*e.g.,* NYSE, NASDAQ) use both continuous time trading during open hours, and a call market before and during open hours to establish an opening price and a closing price. After early experiments at implementing continuous time trading on Ethereum (*e.g.,* EtherDelta, OasisDEX), it was generally accepted that conventional trading is infeasible on Ethereum for performance reasons. Centralized exchanges continued their predominance, while slowly some exchanges moved partial functionality on-chain (*e.g.,* custody of assets) while executing trades off-chain.

A clever quote-driven alternative, called an automatic market maker (AMM), was developed that only requires data structures and traversals with low gas

complexity. This approach has undesirable price dynamics (*e.g.,* market impact of a trade, slippage between the best bid/ask and actual average execution price, *etc.*) which explains why there is no Wall Street equivalent, however, it is efficient on Ethereum and works 'good enough' to attract trading. First generation AMMs provide makers (called liquidity providers) with no ability to act on price information—they are uninformed traders that can only lose (called impermanent loss) on trades but make money on fees. Current generation AMMs (*e.g.,* Uniswap v3) provided informed makers with a limited ability (called concentrated liquidity) to act on proprietary information [32] without breaking Ethereum's performance limitations. Ironically, the logical extension of this is a move back to where it all started—a full-fledged order-driven exchange that allows informed makers the fullest ability to trade strategically.

Contributions. In this paper, we experiment with on-chain markets to understand in detail if they remain infeasible on Ethereum and what the limiting factors are. Some highlights from our research include answering the following questions:

- What type of exchange has the fairest price execution on balance? (A call market.)
- How many orders can be processed on-chain? (Upper-bounded by 152 per block.)
- How much efficiency can be squeezed from diligently choosing the best data structures? (Somewhat limited; turn 38 trades into 152.)
- To what extent can we mitigate front-running attacks? (Almost entirely.)
- Can we stop the exchange's storage footprint on Ethereum from bloating? (Yes, but it is so expensive that it is not worth it.)
- Are on-chain order books feasible on layer 2? (Yes! Optimistic roll-ups reduce gas costs by 99.88%.)
- Which aspects of Ethereum were encountered that required deeper than surface-level knowledge to navigate? (Optimizing gas refunds, Solidity is not truly object-oriented, miner extractable value (MEV) can be leveraged for good, and bridging assets for layer 2.)
- How hard is an on-chain exchange to regulate? (The design leaves almost no regulatory hooks beyond miners (and sequencers on layer 2).)

2 Preliminaries

2.1 Ethereum

We assume the reader is familiar with the following concepts: blockchain technology; smart contracts and decentralized applications (DApps) on Ethereum; how Ethereum transactions are structured, broadcast, and finalized; the gas model including the gas limit (approximately 11M gwei at the time of our experiments) per block. A **gas refund** is a more esoteric subject (not covered thoroughly in any academic work to our knowledge) that we use heavily in our optimizations. Briefly, certain EVM operations (`SELFDESTRUCT` and `SSTORE 0`) cost negative

Type	Description	Advantages	Disadvantages
Centralized Exchanges (CEX)	Order-driven exchange acts as a trusted third party (*e.g.,* Binance, Bitfinex)	Conventional Highest performance Low fees Easy to regulate Low price slippage Verbose trading strategies	Fully trusted custodian Slow withdrawals Server downtime Uncertain fair execution
Partially On-chain Exchange	Order-driven exchange acts as a semi-trusted party (*e.g.,* EtherDelta, 0x, IDEX, Loopring)	High performance Low fees Easy to regulate Low price slippage Verbose trading strategies Semi-custodial	Slow withdrawals Server downtime Front-running attacks Uncertain fair execution
On-Chain Dealers	Quote-driven decentralized exchange trades from inventory with public pricing rule (*e.g.,* Uniswap v3)	Non-custodial Instant trading Moderate performance Fair execution	Unconventional Impermanent loss High price slippage Intrinsic fees Front-running attacks Limited trading strategies Hard to regulate
On-chain Order-Driven Exchanges	Order-driven decentralized exchange executes trades between buyers and sellers (*e.g.,* Lissy)	Conventional Non-custodial Low price slippage Fair execution Verbose trading strategies Front-running is mitigable	Very low performance Hard to regulate

Table 1: Comparison among different trade execution systems.

gas, with the follow caveats: the refund is capped at 50% of the total gas cost of the transaction, and (2) the block gas limit applies to the pre-refunded amount (*i.e.,* a transaction receiving a full refund can cost up to 5.5M gas with an 11M limit). We provide full details of all of these topics in the full version [29].

2.2 Trade Execution Systems

Table 1 illustrates various trade execution systems and summarizes their advantages and disadvantages. A full justification for the table can be found in [29]. Briefly, fully decentralized, on-chain exchanges require the lowest trust, provide instant settlement, and have transparent trading rules that will always execute correctly. Front-running attacks (see Section 5 for a very thorough discussion) are weaknesses inherent in blockchains that require specific mitigation.

2.3 Related Work

Call markets are studied widely in finance and provide high integrity prices (*e.g.,* closing prices that are highly referenced and used in derivative products) [20,31,15]. They can also combat high frequency trading [7,1]. An older 2014 paper [12] on the 'Princeton prediction market' [6] show that call markets mitigate most blockchain-based front-running attacks present in an on-chain continuous-trading exchange as well as other limitations: block intervals are slow and not continuous, there is no support for accurate time-stamping, transactions can be dropped or reordered by miners, and fast traders can react to submitted orders/cancellations when broadcast to network but not in a block and have

Operation	Description
depositToken()	Deposits ERC20 tokens in Lissy smart contract
depositEther()	Deposits ETH in Lissy smart contract
openMarket()	Opens the market
closeMarket()	Closes the market and processes the orders
submitBid()	Inserts the upcoming bids inside the priority queue
submitAsk()	Inserts the upcoming asks inside the priority queue
claimTokens()	Transfers tokens to the traders
claimEther()	Transfers ETH to the traders

Table 2: Primary operations of Lissy smart contract.

their orders appear first. The paper does not include an implementation, was envisioned as running on a custom blockchain (Ethereum was still in development in 2014) and market operations are part of the blockchain logic.

The most similar academic work to this paper is the Ethereum-based periodic auction by Galal *et al.* [16] and the continuous-time exchange TEX [23]. As with us, front-running is a main consideration of these works. In a recent SoK on front-running attacks in blockchain [14], three general mitigations are proposed: confidentiality, sequencing, and design. Both of these papers use confidentiality over the content of orders (*cf.* [38,40,39,10,27]). The main downside is that honest traders cannot submit their orders and leave, they must interact in a second round to reveal their orders. The second mitigation approach is to sequence transactions according to some rule akin to first-in-first-out [22,25]. These are not available for experimentation on Ethereum yet (although Chainlink has announced an intention[1]). The third solution is to design the service in a way that front-running attacks are not profitable—this is the approach with Lissy which uses *no cryptography* and is *submit-and-go* for traders. A detailed comparison of front-running is provided in Section 5. Our paper also emphasizes implementation details: Galal *et al.* do not provide a full implementation, and TEX uses both on-chain and off-chain components, and thus does not answer our research question of how feasible an on-chain order book is.

3 Call Market Design

A call market opens for traders to submit bids and asks which are enqueued until the market closes. Trades are executed by matching the best priced bid to the best priced ask until the best bid is less than the best ask, then all remaining trades are discarded. See [29] for a numeric example. If Alice's bid of $100 is executed against Bob's ask of $90, Alice pays $100, Bob receives $90 and the $10 difference (called a price improvement) is given to miners for reasons in explained in the front-running evaluation (Section 5).

For our experiments and measurements, we implement a call market from scratch. Lissy will open for a specified period of time during which it will accept a capped number of orders (*e.g.,* 100 orders—parameterized so that all orders

[1] A. Juels. blog.chain.link, 11 Sep 2020.

can be processed), and these orders are added to a priority queue (discussed in Section 3.1). Our vision is the market would be open for a very short period of time, close, and then reopen immediately (*e.g.,* every other block). Lissy is open source and written in 336 lines (SLOC) of Solidity plus the priority queue (*e.g.,* we implement 5 variants, each around 300 SLOC). We tested it with the Mocha testing framework using Truffle [37] on Ganache-CLI [36] to obtain our performance metrics. Once deployed, the bytecode of Lissy is 10,812 bytes plus the constructor code (6,400 bytes) which is not stored. The Solidity source code for Lissy and Truffle test files are available in a GitHub repository.[2] We have also deployed Lissy on Ethereum's testnet Rinkeby with flattened (single file) source code of just the Lissy base class and priority queue implementations. It is visible and can be interacted with here: [etherscan.io]. We cross-checked for vulnerabilities with *Slither*[3] and *SmartCheck*[4] and it only fails some 'informational' warnings that are intentional design choices (*e.g.,* a costly loop). All measurements assume a block gas limit of 11 741 495 and 1 gas = 56 Gwei.[5] Table 2 summarizes Lissy's primary operations.

3.1 Priority Queues

In designing Lissy within Ethereum's gas model, performance is the main bottleneck. For a call market, closing the market and processing all the orders are the most time-consuming steps. Assessing which data structures will perform best is hard (*e.g.,* gas refunds, a relatively cheap mapping data structure, only partial support for object-oriented programming) without actually deploying and evaluating several variants.

We first observe that orders are executed in order: highest to lowest price for bids, and lowest to highest price for asks. This means random access to the data structure holding the orders is unnecessary (we discuss cancelling orders later in Section 6.2). We can use a lightweight *priority queue* (PQ) which has only two functions: Enqueue() inserts an element into the priority queue; and Dequeue() removes and returns the highest priority element. Specifically, we use two PQs—one for bids, where the highest price is the highest priority, and one for asks, where the lowest price is the highest priority.

As closing the market is very expensive with any PQ, we rule out sorting the elements while dequeuing and sort during each enqueue. We then implement the following 5 PQ variants:

1. **Heap with Dynamic Array.** A heap is a binary tree where data is stored in nodes in a specific order where the root always represents the highest priority item (*i.e.,* highest bid price/lowest ask price). Our heap stores its data in a Solidity-provided dynamically sized array. The theoretical time complexity is logarithmic enqueue and logarithmic dequeue.

[2] Github: Link removed for anonymity.
[3] https://github.com/crytic/slither
[4] https://tool.smartdec.net
[5] EthStats (July 2020): `https://ethstats.net/`

2. **Heap with Static Array.** This variant replaces the dynamic array with a Solidity storage array where the size is statically allocated. This is asymptotically the same and marginally faster in practice.
3. **Heap with Mapping.** In this variant, we store a key for the order in the heap instead of the entire order. Once a key is dequeued, the order struct is drawn from a Solidity mapping (which stores key-value pairs very efficiently). This is asymptotically the same and faster with variable-sized data.
4. **Linked List.** In this variant, elements are stored in a linked list (enabling us to efficiently insert a new element between two existing elements during enqueue). Solidity is described as object-oriented but the Solidity equivalent of an object is an entire smart contract. Therefore, an object-oriented linked list must either (1) create each node in the list as a struct—but this is not possible as Solidity does not support recursive structs—or (2) make every node in the list its own contract. The latter option seems wasteful and unusual, but it surprisingly ends up being the most gas efficient data structure to dequeue. The theoretical time complexity is linear enqueue and constant dequeue.
5. **Linked List with Mapping.** Finally, we try a variant of a linked list using a Solidity mapping. The value of the mapping is a struct with the incoming order's data and the key of the next (and previous) node in the list. The contract stores the key of the first node (head) and last node (tail) in the list. Asymptotically, it is linear enqueue and constant dequeue.

We implemented, deployed, and tested each PQ. A simple test of enqueuing 50 integers chosen at random from a fixed interval is in Figure 1 and dequeing them all is in Table 3. Dequeuing removes data from the contract's storage resulting in a gas refund. Based on our manual estimates,[6] every variant receives the maximum gas refund possible (*i.e.,* half the total cost of the transaction). In other words, each of them actually consumes twice the `gasUsed` amount in gas before the refund. However, none of them are better or worse based on how much of a refund they generate.

We observe that (1) the linked list variants are materially cheaper than the heap variants at dequeuing; (2) dequeuing in a call market must be done as a batch, whereas enqueuing is paid for one at a time by the trader submitting the order; and (3) Ethereum will not permit more than hundreds of orders so asymptotic behaviour is not significant. For these reasons, we suggest using one of the linked list variants. As it can be seen in Figure 1, the associated cost for inserting elements into a linked list PQ is significantly greater than the linked list with mapping, as each insertion causes the creation of a new contract. Accordingly, we choose to implement the call market with the linked list with mapping which balances a moderate gas cost for insertion (*i.e.,* order submission) with one for removal (*i.e.,* closing the market and matching the orders). In Section 4, we implement Lissy on Layer 2. There, the PQ variant does not change the layer

[6] EVM does not expose the refund counter. We determine how many storage slots are being cleared and how many smart contracts destroyed, then we multiply these numbers by 24,000 or 15,000 respectively.

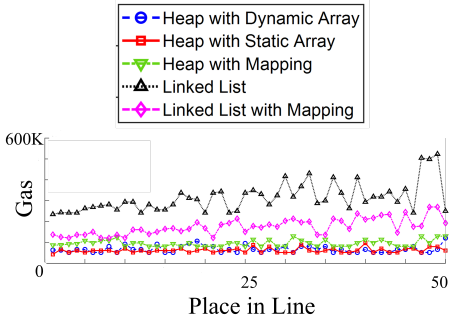

Fig. 1: Gas costs for enqueuing 50 random integers into five priority queue variants. For the x-axis, a value of 9 indicates it is the 9th integer entered in the priority queue. The y-axis is the cost of enqueuing in gas.

	Gas Used	*Refund*	*Full Refund?*
Heap with Dynamic Array	2,518,131	750,000	●
Heap with Static Array	1,385,307	750,000	●
Heap with Mapping	2,781,684	1,500,000	●
Linked List	557,085	1,200,000	●
Linked List with Mapping	731,514	3,765,000	●

Table 3: The gas metrics associated with dequeuing 50 integers from five priority queue variants. Full refund amount is shown but the actual refund that is applied is capped.

	Gas Used	*Potential Refund*	*Full Refund?*
Linked List without `SELFDESTRUCT`	721,370	0	◐
Linked List with `SELFDESTRUCT`	557,085	1,200,000	●
Linked List with Mapping and without `DELETE`	334,689	765,000	●
Linked List with Mapping and `DELETE`	731,514	3,765,000	●

Table 4: The gas metrics associated with dequeuing 50 integers from four linked list variants. For the refund, (●) indicates the refund was capped at the maximum amount and (◐) means a greater refund would be possible.

1 gas costs (as calldata size is the same) and the number of orders can be substantially increased. thus, we reconsider asymptotic and choose a heap (with dynamic array) to lower L2 gas costs across both enqueuing and dequeuing.

3.2 Cost/Benefit of Cleaning Up After Yourself

One consequence of a linked list is that a new contract is created for every node in the list. Beyond being expensive for adding new nodes (a cost that will be bared by the trader in a call market), it also leaves a large footprint in the active Ethereum state, especially if we leave the nodes on the blockchain in perpetuity (*i.e.,* we just update the head node of the list and leave the previous head 'dangling'). However in a PQ, nodes are only removed from the head of the list; thus the node contracts could be 'destroyed' one by one using an extra operation, `SELFDESTRUCT`, in the `Dequeue()` function. As shown in Table 4, the refund from doing this outweighs to the cost of the extra computation: gas costs are reduced from 721K to 557K. This suggests a general principle: cleaning up after yourself

	Max Trades (w.c.)	Gas Used for Max Trades	Gas Used for 1000 Trades	Gas Used for Submission (avg)
Heap with Dynamic Array	38	5,372,679	457,326,935	207,932
Heap with Static Array	42	5,247,636	333,656,805	197,710
Heap with Mapping	46	5,285,275	226,499,722	215,040
Linked List	152	5,495,265	35,823,601	735,243
Linked List with Mapping	86	5,433,259	62,774,170	547,466

Table 5: Performance of Lissy for each PQ variant. Each consumes just under the block gas limit (∼11M gas) with a full refund of half of its gas.

will pay for itself in gas refunds. Unfortunately, this is not universally true as shown by applying the same principle to the linked list with mapping.

Dequeuing in a linked list with mapping can be implemented in two ways. The simplest approach is to process a node, update the head pointer, and leave the 'removed' node's data behind in the mapping untouched (where it will never be referenced again). Alternatively, we can call `DELETE` on each mapping entry once we finish processing a trade. As it can be seen in the last two rows of Table 4, leaving the data on the blockchain is cheaper than cleaning it up.

The lesson here is that gas refunds incentivize developers to clean up storage variables they will not use again, but it is highly contextual as to whether it will pay for itself. Further, the cap on the maximum refund means that refunds are not fully received for large cleanup operations (however removing the cap impacts the miners' incentives to include the transaction). We present a second case study of the cost-benefit of clearing a mapping when it is no longer needed (including our idea to store the mapping in its own contract so it can `SELFDESTRUCT` with a single function call) in [29]. The unfortunate takeaway is, again, that it is cheapest to leave the mapping in place. Cleaning up EVM state is a complicated and under-explored area of Ethereum in the research literature. For our own work, we strive to be good citizens of Ethereum and clean up to the extent that we can—thus all PQs in Table 3 implement some cleanup.

3.3 Lissy Performance Measurements

The main research question is how many orders can be processed under the Ethereum block gas limit. The choice of PQ implementation is the main influence on performance and the results are shown in Table 5. These numbers are for the *worst-case*—when every submitted bid and ask is marketable (*i.e.,* will require fulfillment). In practice, once `closeMarket()` hits the first bid or ask that cannot be executed, it can stop processing all remaining orders. Premised on Ethereum becoming more efficient over time, we were interested in how much gas it would cost to execute 1000 pairs of orders, which is given in the third column. The fourth column indicates the cost of submitting a bid or ask — since this cost

will vary depending on how many orders are already submitted (recall Figure 1), we average the cost of 200 order submissions.

The main takeaway is that call markets appear to be limited to processing about a hundred orders per transaction and even that is at the enormous cost of monopolizing an entire Ethereum block just to close the market. Perhaps Lissy can work today in some circumstances like very low liquidity tokens, or markets with high volumes and a small number of traders (*e.g.,* liquidation auctions).

4 Lissy on Arbitrum

Layer 2 (L2) solutions [18] are a group of scaling technologies proposed to address specific drawbacks of executing transactions on Ethereum, which is considered *Layer 1 (L1)*. Among these proposals, *roll-ups* prioritize reducing gas costs (as opposed to other valid concerns like latency and throughput, which are secondary for Lissy). We review two variants, *optimistic roll-ups* and *zk roll-ups*, in [29]. Briefly, in a roll-up, every transaction is stored (but not executed) on Ethereum, then executed off-chain, and the independently verifiable result is pushed back to Ethereum, with some evidence of being executed correctly. We also compare Lissy on Arbitrum to Loopring 3.0 in [29].

We choose to experiment with Lissy on the optimistic rollup Arbitrum.[7] To deploy a DApp on Arbitrum, or to execute a function on an existing Arbitrum DApp, the transaction is sent to an *inbox* on L1. It is not executed on L1, it is only recorded (as calldata) in the inbox. An open network of *validators* watch the inbox for new transactions. Once inbox transactions are finalized in an Ethereum block, validators will execute the transactions and assert the result of the execution to other validators on a sidechain called ArbOS. As the Inbox contract maintains all Arbitrum transactions, anyone can recompute the entire current state of the ArbOS and file a dispute if executions are not correctly reported on ArbOS. Disputes are adjudicated by Ethereum itself and require a small, constant amount of gas, invariant to how expensive the transaction being disputed is. When the dispute challenge period is over, the new state of ArbOS is stored as a checkpoint on Ethereum.

4.1 Lissy Performance Measurements on Arbitrum

Testing Platforms. We implement Lissy using the Arbitrum Rollup chain hosted on the Rinkeby testnet. It is visible and can be interacted with here: [Arbitrum Explorer]. To call functions on Lissy, traders can (1) send transactions directly to the Inbox contract, or (2) use a relay server (called a *Sequencer*) provided by the Arbitrum. The sequencer will group, order, and send all pending transactions together as a single Rinkeby transaction to the Inbox (and pays the gas).

In our Lissy variant on Arbitrum, the validators do all computations (both enqueuing and dequeuing) so we choose to use a heap with dynamic array for

[7] See `https://offchainlabs.com` for more current details than the 2018 *USENIX Security* paper [21].

	Layer1 gasUsed	**Layer2 ArbGas**
Lissy on Ethereum	5,372,679	N/A
Lissy on Arbitrum	6,569	508,250

Table 6: Gas costs of closing a market on Ethereum and on Arbitrum. ArbGas corresponds to Layer 2 *computation used*.

our priority queue, which balances the expense of both operations. Heaps are 32% more efficient than linked lists for submitting orders and 29% less efficient for closing. Recall that without a roll-up, such a priority queue can only match 38 pairs at a cost of 5,372,679 gas. Table 6 shows that 38 pairs cost only 6,569 in L1 gas (a 99.88% savings). This is the cost of submitting the `closeMarket()` transaction to the Inbox to be recorded, which is 103 bytes of calldata. Most importantly, recording `closeMarket()` in the Inbox will always cost around 6,569 even as the number of trades increases from 38 pairs to thousands or millions of pairs. Of course, as the number of trades increase, the work for the validators on L2 increases, as measured in ArbGas. The price of ArbGas in Gwei is not well established but is anticipated to be relatively cheap. Arbitrum also reduces the costs for traders to submit an order: from 207,932 to 6,917 in L1 gas. We illustrate the interaction between the traders and Lissy on Arbitrum including bridges, inboxes, sequencers and validators in [29].

Running Lissy on Arbitrum has one large caveat. If the ERC20 tokens being traded are not issued on ArbOS, which is nearly always the case today, they first need to be *bridged* onto ArbOS, as does the ETH. Traders send ETH or tokens to Arbitrum's bridge contracts which create the equivalent amount at the same address on L2. Withdrawals work the same way in reverse, but are only final on L1 after a dispute challenge period (currently 1 hour).[8]

5 Front-running Evaluation

As we illustrate in Table 7, call markets have a unique profile of resilience against *front-running attacks* [12,14,13] that differs somewhat from continuous-time markets and automated market makers. Traders are sometimes distinguished as *makers* (adds orders to a market) and *takers* (trades against a pre-existing, unexecuted orders). A continuous market has both. All traders using an automated market maker are takers, while the investors who provide tokens to the AMM (liquidity providers) are makers. Under our definition, a call market only has makers: the only way to have a trade executed is to submit an order. The front-running attacks in Table 7 are subcategorized, using a recent SoK [14], as being *Insertion*, *Displacement*, and *Suppression*. To explain the difference, we will illustrate the first three attacks in the table.

[8] L1 users might accept assets before they are finalized as they can determine their eventual emergence on L1 is indisputable (*eventual finality*).

			Centralized Continuous Market (Coinbase)	Partially Off-chain Continuous Market (EtherDelta)	Partially Off-chain Continuous Market w/ Roll-up (Loopring)	On-chain Continuous Market (OasisDex)	On-chain Dark Continuous Market (TEX)	On-chain Automated Market Maker (Uniswap)	On-chain Call Market w/ Price Improvement	On-chain Call Market (**Lissy**)	On-chain Call Market w/ Roll-up (**Lissy** variant)	On-chain Dark Call Market (Galal *et al.*)
Who is Mallory? Authority, Trader, Miner, Sequencer			A	A,T,M	A,T,M,S	T,M	T,M	T,M	T,M	T,M	T,M,S	T,M
Attack Example	Mallory (*maker*) squeezes in a transaction before Alice's (*taker*) order	Ins.	○	○	○	○	●	○	●	●	●	●
	Mallory (*taker*) squeezes in a transaction before Bob's (*taker 2*)	Disp.	○	○	○	○	●	○	●	●	●	●
	Mallory (*maker 1*) suppresses a better incoming order from Alice (*maker 2*) until Mallory's order is executed	Supp.	○	○	○	●	●	●	◐	◐	◐	◐
	A hybrid attack based on the above (*e.g.,* sandwich attacks, scalping)	I/S/D	○	○	○	○	●	○	○	●	●	●
	Mallory suspends the market for a period of time	Supp.	○	○	○	◐	◐	◐	◐	◐	◐	◐
	Spoofing: Mallory (*maker*) puts an order as bait, sees Alice (*taker*) tries to execute it, and cancels it first	S&D	○	○	○	○	●	○	●	●	●	●
	Cancellation Griefing: Alice (*maker*) cancels an order and Mallory (*taker*) fulfills it first	Disp.	○	○	○	○	●	○	●	●	●	●

Table 7: An evaluation of front-running attacks (rows) for different types of order books (columns). Front-running attacks are in three categories: Insertion, displacement, and suppression. A full dot (●) means the front-running attack is mitigated or not applicable to the order book type, a partial mitigation (◐) is awarded when the front-running attack is possible but expensive, and we give no award (○) if the attack is feasible.

In an *insertion attack*, Mallory learns of a transaction from Alice. Consider Alice submitting a bid order for 100 tokens at any price (market order). Mallory decides to add new ask orders to the book (limit orders) at the maximum price reachable by Alice's order given the rest of the asks in the book. Mallory must arrange for her orders to be added before Alice's transaction and then arrange for Alice's transaction to be the next (relevant) transaction to run (*e.g.,* before competing asks from other traders are added).

In a centralized exchange, Mallory would collude with the *authority* running the exchange to conduct this attack. On-chain, Mallory could be a fast *trader* who sees Alice's transaction in the mempool and adds her transaction with a higher gas fee to bribe miners to execute hers first (insertion is probabilist and not guaranteed). Finally, Mallory could be the *miner* of the block that includes Alice's transaction allowing her to insert with high fidelity. Roll-ups use *sequencers* discussed in Section 5.1.

A *displacement attack* is like an insertion attack, except Mallory does not care what happens to Alice's original transaction—she only cares about being first. If Mallory sees Alice trying to execute a trade at a good price, she could try to beat Alice and execute the trade first. Mallory is indifferent to whether Alice can then execute her trade or not. The analysis of both insertion and suppression

attacks are similar. Call markets mitigate these basic insertion and displacement attacks because they do not have any time priority (e.g., if you were to shuffle the order of all orders submitted within the same call, the outcome would be exactly the same). A different way to mitigate these attacks is to seal orders with confidentiality (a *dark* market).

In a *suppression attack*, Mallory floods the network with transactions until a trader executes her order. Such selective denial of service is possible by an off-chain operator. With on-chain continuous markets, it is not possible to suppress Alice's transaction while also letting through a transaction from a taker—suppression applies to all Ethereum transactions or none. A call market is uniquely vulnerable because it eventually times out (which does not require an on-chain transaction) and new orders cannot be added. We still award a call market partial mitigation since suppression attacks are expensive (*cf.* Fomo3D attack [14]). If the aim of suppression is a temporary denial of service (captured by attack 5 in the table), then all on-chain markets are vulnerable to this expensive attack.

Some attacks combine more than one insertion, displacement, and/or suppression attacks. AMMs are vulnerable to a double insertion called a sandwich attack [42] which bookends a victim's trade with the front-runner's trades (plus additional variants). In a traditional call market, a market clearing price is chosen and all trades are executed at this price. All bids made at a higher price will receive the assets for the lower clearing price (and conversely for lower ask prices): this is called a *price improvement* and it allows traders to submit at their best price. A hybrid front-running attack allows Mallory to extract any price improvements. Consider the case where Alice's ask crosses Bob's bid with a material price improvement. Mallory inserts a bid at Alice's price, suppresses Bob's bid until the next call, and places an ask at Bob's price. She buys and then immediately sells the asset and nets the price improvement as arbitrage. To mitigate this in Lissy, all price improvements are given to the miner (using `block.coinbase.transfer()`). This does not actively hurt traders—they always receive the same price that they quote in their orders—and it removes any incentive for miners to front-run these profits.

Other front-running attacks use order cancellations (see Section 6.2) which Lissy mitigates by running short-lived markets with no cancellations.

There are two main takeaways from Table 7. Call markets provide strong resilience to front-running only bested slightly by dark markets like TEX [23], however, they do it through design—no cryptography and no two-round protocols. A second observation is that dark call markets, like Galal *et al.* [16], are no more resilient to front-running than a lit market (however confidentiality could provide resilience to predatory trading algorithms that react quickly to trades without acutally front-running).

5.1 Front-running on Arbitrum

In our Lissy variant on the Arbitrum, traders can submit transactions to the Layer 1 Inbox contract instead of directly to the Lissy DApp. This has the same

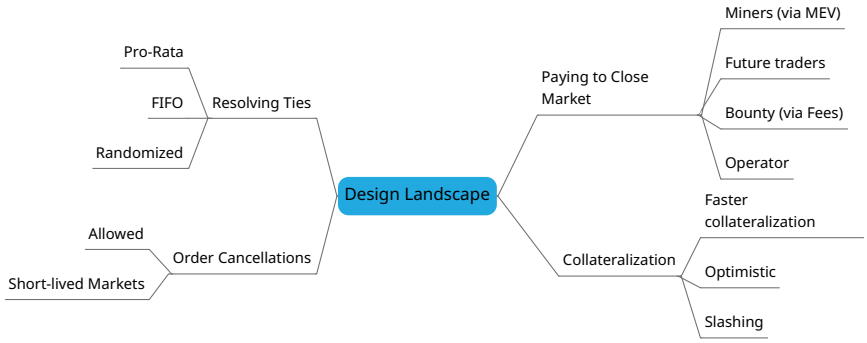

Fig. 2: A design landscape for on-chain call markets.

front-running profile as Lissy itself; only the Layer 1 destination address is different. If a sequencer is mandatory, it acts with the same privilege as a Layer 1 Ethereum miner in ordering the transactions it receives. Technically, sequencers are not limited to roll-ups and could be used in the context of normal Layer 1 DApps, but they are more apparent in the context of roll-ups. A sequencer could be trusted to execute transactions in the order it receives them, outsource to a fair ordering service, or (in a tacit acknowledge of the difficulties of preventing front-running) auction off permission to order transactions to the highest bidder (called a *MEV auction*). As shown in Table 7, a sequencer is an additional front-running actor but does not otherwise change the kinds of attacks that are possible.

6 Design Landscape

Lissy is a simple base class that implements the core functionality of a call market. To use it in the real world, design decisions need to be made about how it will be used. Figure 2 provides a design landscape for Lissy deployment, with possible extensions and customization.

6.1 Token Divisibility and Ties

A common trading rule is to fill ties in proportion to their volume (*i.e., pro rata* allocation)[9]. This can fail when tokens are not divisible. Consider the following corner case: 3 equally priced bids of 1 non-divisible token and 1 ask at the same price: (1) the bid could be randomly chosen (*cf.* Libra [28]), or (2) the bid could be prioritized based on time. In Lissy, tokens are assumed to be divisible.

[9] If Alice and Bob bid the same price for 100 tokens and 20 tokens respectively, and there are only 60 tokens left in marketable asks, Alice receives 50 and Bob 10.

If the volume of the current best bid does not match the best ask, the larger order is partially filled and the remaining volume is considered against the next best order. We note the conditions under which pro rata allocation fails (*i.e.,* non-divisible assets, an exact tie on price, and part of the final allocation) are improbable. (1) is the fairest solution with one main drawback: on-chain sources of 'randomness' are generally deterministic and manipulatable by miners [5,9], while countermeasures can take a few blocks to select [4]. We implement (2) which means front-running attacks are possible in this one improbable case.

6.2 Order Cancellations

Support for cancellation opens the market to new front-running issues where other traders (or miners) can displace cancellations until after the market closes. However, one benefit of a call market is that beating a cancellation with a new order has no effect, assuming the cancellation is run any time before the market closes. Also, cancellations have a performance impact. Cancelled orders can be removed from the underlying data structure or accumulated in a list that is cross-checked when closing the market. Removing orders requires a more verbose structure than a priority queue (*e.g.,* a self-balancing binary search tree instead of a heap; or methods to traverse a linked list rather than only pulling from the head). Lissy does not support order cancellations. We intend to open and close markets quickly (on the order of blocks), so orders are relatively short-lived.

6.3 Who Pays to Close/Reopen the Market?

In the Princeton paper [12], the call market is envisioned as an alt-coin, where orders accumulate within a block and a miner closes the market as part of the logic of producing a new block (*i.e.,* within the same portion of code as computing their coinbase transaction in Bitcoin or `gasUsed` in Ethereum). In Lissy, someone needs to execute `closeMarket()` at the right time and pay for it, which is probably the most significant design challenge for Lissy.

Since price improvements are paid to the miners, the miner is incentivized to run `closeMarket()` if it pays for itself. Efficient algorithms for miners to automatically find 'miner extractable value (MEV)' opportunities [13] is an open research problem. Even if someone else pays to close the market, MEV smooths out some market functionality. Assume several orders are submitted and then `closeMarket()`. A naive miner might order the `closeMarket()` before the submitted orders, effectively killing those orders and hurting its own potential profit. MEV encourages miners to make sure a profitable `closeMarket()` in the mempool executes within its current block (to claim the reward for itself) and that it runs after other orders in the mempool to maximize its profit.

Without MEV, markets should open and close on different blocks. In this alternative, the `closeMarket()` function calls `openMarket()` as a subroutine and sets two modifiers: orders are only accepted in the block immediately after the current block (*i.e.,* the block that executes the `closeMarket()`) and `closeMarket()` cannot be run again until two blocks after the current block.

Another option is to have traders in the next call market pay to incrementally close the current market. For example, each order in the next market needs to pay to execute the next x orders in the current market until the order book is empty. This has two issues: first, amortizing the cost of closing the market amongst the early traders of the new market disincentives trading early in the market; the second issue is if not enough traders submit orders in the new market, the old market never closes (resulting in a backlog of old markets waiting to close).

A closely related option is to levy a carefully computed fee against the traders for every new order they submit. These fees are accumulated by the DApp to use as a bounty. When the time window for the open market elapses, the sender of the first `closeMarket()` function to be confirmed receives the bounty. This is still not perfect: `closeMarket()` cost does not follow a tight linear increase with the number of orders, and gas prices vary over time which could render the bounty insufficient for offsetting the `closeMarket()` cost. If the DApp can pay for its own functions, an interested party can also arrange for a commercial service (*e.g.,* any.sender[10]) to relay the `closeMarket()` function call on Ethereum (an approach called *meta-transactions*). This creates a regulatory hook.

The final option is to rely on an interested third party (such as the token issuer for a given market) to always close the market, or occasionally bailout the market when one of the above mechanisms fails. An external service like Ethereum Alarm Clock[11] (which also creates a regulatory hook) can be used to schedule regular `closeMarket()` calls.

6.4 Collateralization Options

In Lissy, both the tokens and ETH that a trader wants to potentially use in the order book are preloaded into the contract. We discuss some alternative designs in [29].

7 Concluding Remarks

Imagine you have just launched a token on Ethereum. Now you want to be able to trade it. While the barrier to entry for exchange services is low, it still exists. For a centralized or decentralized exchange, you have to convince the operators to list your token and you will be delayed while they process your request. For an automated market maker, you will have to lock up a large amount of ETH into the DApp, along with your tokens. For roll-ups, you will have to host your own servers. By contrast to all of these, with an on-chain order book, you just deploy the code alongside your token and trading is immediately supported. This should concern regulators. Even if it is too slow today, there is little reason for developers not to offer it as a fallback solution that accompanies every token. With future improvements to blockchain scalability, it could become the de facto trading method.

[10] `https://github.com/PISAresearch/docs.any.sender`
[11] `https://ethereum-alarm-clock-service.readthedocs.io/`

Acknowledgements. The authors thank the AMF (Autorité des Marchés Financiers) for supporting this research project. J. Clark also acknowledges partial funding from the National Sciences and Engineering Research Council (NSERC)/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies, as well as NSERC through a Discovery Grant. M. Moosavi acknowledges support from Fonds de Recherche du Québec - Nature et Technologies (FRQNT).

References

1. M. Aquilina, E. B. Budish, and P. O'Neill. Quantifying the high-frequency trading "arms race": A simple new methodology and estimates. *Chicago Booth Research Paper*, (20-16), 2020.
2. E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev. Scalable zero knowledge with no trusted setup. In *CRYPTO*, 2019.
3. E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In *CRYPTO*, 2013.
4. D. Boneh, J. Bonneau, B. Bünz, and B. Fisch. Verifiable delay functions. In *CRYPTO*, 2018.
5. J. Bonneau, J. Clark, and S. Goldfeder. On bitcoin as a public randomness source. `https://eprint.iacr.org/2015/1015.pdf`, 2015. Accessed: 2015-10-25.
6. R. Brandom. This princeton professor is building a bitcoin-inspired prediction market, Nov 2013.
7. E. Budish, P. Cramton, and J. Shim. The high-frequency trading arms race: Frequent batch auctions as a market design response. *The Quarterly Journal of Economics*, 130(4):1547–1621, 2015.
8. J. V. Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution. In *USENIX Security Symposium*, Baltimore, MD, Aug. 2018. USENIX Association.
9. B. Bünz, S. Goldfeder, and J. Bonneau. Proofs-of-delay and randomness beacons in ethereum. In *IEEE S&B*, 2017.
10. J. Cartlidge, N. P. Smart, and Y. Talibi Alaoui. Mpc joins the dark side. In *ASIACCS*, pages 148–159, 2019.
11. R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *IEEE EuroS&P*, pages 185–200. IEEE, 2019.
12. J. Clark, J. Bonneau, E. W. Felten, J. A. Kroll, A. Miller, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS*, 2014.
13. P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. In *IEEE Symposium on Security and Privacy*, 2020.
14. S. Eskandari, S. Moosavi, and J. Clark. Sok: Transparent dishonesty: front-running attacks on blockchain. In *WTSC*, pages 170–189. Springer, 2019.
15. E. Félez-Viñas and B. Hagströmer. Do volatility extensions improve the quality of closing call auctions? *Financial Review*, 56(3):385–406, 2021.

16. H. S. Galal and A. M. Youssef. Publicly verifiable and secrecy preserving periodic auctions. In *WTSC*. Springer, 2021.
17. R. Gennaro, C. Gentry, B. Parno, and M. Raykova. Quadratic span programs and succinct nizks without pcps. In *EUROCRYPT*, 2013.
18. L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais. Sok: Layer-two blockchain protocols. In *Financial Cryptography*, pages 201–226. Springer, 2020.
19. L. Harris. *Trading and exchanges: market microstructure for practitioners*. Oxford, 2003.
20. P. Hillion and M. Suominen. The manipulation of closing prices. *Journal of Financial Markets*, 7(4):351–375, 2004.
21. H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten. Arbitrum: Scalable, private smart contracts. In *USENIX Security Symposium*, pages 1353–1370, 2018.
22. M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels. Order-fairness for byzantine consensus. In *CRYPTO*, pages 451–480. Springer, 2020.
23. R. Khalil, A. Gervais, and G. Felley. Tex-a securely scalable trustless exchange. *IACR Cryptol. ePrint Arch.*, 2019:265, 2019.
24. P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. Spectre attacks: Exploiting speculative execution. In *IEEE Symposium on Security and Privacy*, pages 1–19, 2019.
25. K. Kursawe. Wendy, the good little fairness widget: Achieving order fairness for blockchains. In *ACM AFT*, 2020.
26. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. Meltdown: Reading kernel memory from user space. In *USENIX Security Symposium*, pages 973–990, Baltimore, MD, Aug. 2018. USENIX Association.
27. F. Massacci, C. N. Ngo, J. Nie, D. Venturi, and J. Williams. Futuresmex: secure, distributed futures market exchange. In *IEEE Symposium on Security and Privacy*, pages 335–353. IEEE, 2018.
28. V. Mavroudis and H. Melton. Libra: Fair order-matching for electronic financial exchanges. In *ACM AFT*, 2019.
29. M. Moosavi and J. Clark. Lissy: Experimenting with on-chain order books, 2021.
30. A. Norry. The history of the mt gox hack: Bitcoin's biggest heist. `https://blockonomi.com/mt-gox-hack/`, June 2019. (Accessed on 12/31/2019).
31. M. S. Pagano and R. A. Schwartz. A closing call's impact on market quality at euronext paris. *Journal of Financial Economics*, 68(3):439–484, 2003.
32. A. Park. The conceptual flaws of constant product automated market making. *Available at SSRN 3805750*, 2021.
33. H. Ragab, A. Milburn, K. Razavi, H. Bos, and C. Giuffrida. Crosstalk: Speculative data leaks across cores are real. In *IEEE Symposium on Security and Privacy*, 2021.
34. Securities and E. B. of India. Sebi | order in the matter of nse colocation. `https://www.sebi.gov.in/enforcement/orders/apr-2019/order-in-the-matter-of-nse-colocation_42880.html`, 2019. (Accessed on 11/11/2019).
35. C. Signer. Gas cost analysis for ethereum smart contracts. Master's thesis, ETH Zurich, Department of Computer Science, 2018.
36. T. Suite. Ganache. `https://www.trufflesuite.com/ganache`, May 2021. (Accessed on 05/26/2021).

37. T. Suite. Truffle. `https://www.trufflesuite.com/docs/truffle/overview`, May 2021. (Accessed on 05/26/2021).
38. C. Thorpe and D. C. Parkes. Cryptographic securities exchanges. In *Financial Cryptography*, 2007.
39. C. Thorpe and S. R. Willis. Cryptographic rule-based trading. In *Financial Cryptography*, 2012.
40. W. Yuen, P. Syverson, Z. Liu, and C. Thorpe. Intention-disguised algorithmic trading. In *Financial Cryptography*, 2010.
41. L. Zhao, J. I. Choi, D. Demirag, K. R. B. Butler, M. Mannan, E. Ayday, and J. Clark. One-time programs made practical. In *Financial Cryptography*, 2019.
42. L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais. High-frequency trading on decentralized on-chain exchanges. In *IEEE Symposium on Security and Privacy*, 2021.