Supplementary Material For
AUCIL: An Inclusion List Design for Rational Parties

Appendix E.
Proofs for Section 4

Lemma 4. *(Small Mempool) If the mempool contains fewer than k transactions, i.e., $|M| < k$, then any utility maximizing algorithm should assign every transaction to every proposer: $L_i = M$ for all $i \in \{1, \ldots, n\}$.*

Consider to the contrary, $|L_i| < |M|$. In such a case, there exists an object m_j not in the allocation L_i. Since L_i is a subset of M, $|L_i| < k$, and thus the object L_i can be added to the allocation.

Lemma 5. *(Correlated Equilibrium Reduction) If $|M| \geq k$, then any algorithm that satisfies constraint (5) also satisfies the constraint (4).*

Proof. Since $|M| \geq k$, $|L_i| = k$. This is because if $|L_i| < k$, then there exists an object in M, not in L_i, which can be added to increase the utility gained by the selection. Now let's assume, to the contrary, that constraint (5) holds but constraint (4) does not. The negation of constraint (4) states

$$\exists L_i \in L, \exists L_{i'} = M^{[\leq k]} : \mathbb{U}_i(L_i) < \mathbb{U}_i(L_{i'})$$

Let $L_{i'} \neq L_i$ represent the allocation with the highest utility (strictly greater than allocation L_i). If multiple such allocations exist with the highest utility, consider $L_{i'}$ as the set that differs in the least number of objects from L_i. There exists an object m_a such that $m_a \in L_i$ but $m_a \notin L_{i'}$. (If no such object exists, then $L_{i'} \supseteq L_i$. However since $|L_{i'}| \leq k = |L_i|$, this is possible only if $L_i = L_{i'}$)

Consider $|L_{i'}| < k$. Adding m_a would only add to the party's utility; however, $L_{i'}$ was considered as the maximal such allocation, and thus such an $L_{i'}$ can only exist if $|L_{i'}| = k$. Since both $L_{i'}$ and L_i are of size k and there exists $m_a \in L_i$ but $m_a \notin L_{i'}$, there must exist $m_b \in L_{i'}$ but $m_b \notin L_i$.

Given all other selections $L_j \neq L_i$ remain the same as governed by the allocation, the number of times the object m_b is chosen increases by 1 in $L_{i'}$ compared to L_i. From(1),

$$\mathbb{U}_i(L_i) = \mathbb{U}_i(L_i \setminus m_a) + \frac{u_{m_a}}{\widetilde{n_a}}$$
$$\mathbb{U}_i(L_{i'}) = \mathbb{U}_i(L_{i'} \setminus m_b) + \frac{u_{m_b}}{\widetilde{n_b} + \gamma}$$

From constraint(5), in this case (where $\exists i : (L_i \in L, m_a \in L_i, m_b \notin L_i)$),

$$\frac{u_{m_a}}{\widetilde{n_a}} \geq \frac{u_{m_b}}{\widetilde{n_b} + \gamma}$$

Consider the set $L_{i''} = (L_{i'} \setminus \{m_b\}) \cup \{m_a\}$. $|L_{i''}| = |L_{i'}|$, and thus satisfies $M^{[\leq k]}$ property. The utility of this set is

$$\begin{aligned}\mathbb{U}_i(L_{i''}) &= \mathbb{U}_i(L_{i'} \setminus m_b) + \frac{u_{m_a}}{\widetilde{n_a}} \\ &= \mathbb{U}_i(L_{i'}) + \frac{u_{m_a}}{\widetilde{n_a}} - \frac{u_{m_b}}{\widetilde{n_b} + \gamma} \\ &\geq \mathbb{U}_i(L_{i'})\end{aligned}$$

This is a contradiction since $L_{i'}$ was considered as the set with the highest utility that differed in the least elements compared to L_i; however, we show the existence of another set with one less element differing from L_i, which has a utility greater than or equal to $L_{i'}$. □

Theorem 2. (Correlated Equilibrium) *Given the assignment of input lists $L = \{L_1, \ldots, L_n\}$ according to algorithm 1, then following the strategy $\Psi = \{\Psi_1, \ldots, \Psi_n\}$, where $\Psi_i =$ select L_i, is a correlated equilibrium, i.e., for all parties $P_i \in N$, P_i cannot obtain a better utility from selecting any other list than L_i given every other party P_j follows $\Psi_j =$ select L_j.*

Proof. To prove the theorem statement, we first prove that Eq(5) holds for Algorithm 1. Let $U(m_i, r)$ represent the utility from object m_i in round r of the selection. Let $O(r)$ represent the object chosen by the algorithm in round r. Let $R(m_i)$ represent the last round in which m_i was chosen (For objects never chosen, this value is not defined). Let $N_c(m_i, r)$ represent the expected number of times object m_i has been selected by round r (considering that with probability $1 - \gamma$ the object might be dropped)[This value is γ less than the corresponding N_c value in the algorithm]. At the end of round $r = n \cdot k$, $T(M) = S$ and utility from each $O(r)$ is $U(O(r), R(O(r)))$, i.e., the utility value it had on its last selection. Note that

$$r_1 < r_2 \implies U(m_i, r_1) \geq U(m_i, r_2) \tag{10}$$

That is, the utility of an object can only decrease or remain the same as the rounds progress.

Also, note that

$$U(m_i, r_1) \geq U(m_i, r_2) \tag{11}$$

Rewriting Eq (5) in these new terms, we have

$$\begin{aligned}&\forall r, m_i \in M : \exists j : (L_j \in L,\ O(r) \in L_j, m_i \notin L_j) \\ &\implies U(O(r), R(O(r))) \geq \frac{u_{m_i}}{N_c(m_i, n \cdot k) + \gamma}\end{aligned}$$

We claim that no matter what the allocation rule is, after the choice of the selection algorithm (Step 2), the resulting allocation always satisfies this equation, as long as an object is not allocated to the same party twice. In other words, we will prove the following stronger statement

$$\begin{aligned}&\forall r \in \{1, \ldots, n \cdot k\},\ m_i \in M : \\ &\exists j : m_i \notin L_j \implies U(O(r), R(O(r))) \geq \frac{u_{m_i}}{N_c(m_i, n \cdot k) + \gamma}\end{aligned}$$

We prove this by contradiction. Let's assume, to the contrary, that for some m_i and some $O(r) \neq m_i$, such that $\exists j : m_i \notin L_j$,

$$U(O(r), R(O(r))) < \frac{u_{m_i}}{N_c(m_i, n \cdot k) + \gamma} \tag{12}$$

Since $m_i \notin L_j$ for at least some party, and we are assuming that the same object is not allocated to the same party twice, the number of times m_i has been chosen must be less than n implying that $N_c(m_i, n \cdot k) < n\gamma + 1 - \gamma$. This means that line 10 never triggers for m_i.

Case 1: For all $m_i \neq O(n \cdot k)$, the R.H.S. of (12) corresponds to the utility of object m_i in round $n \cdot k$, i.e., $U(m_i, n \cdot k)$. Thus, we are given,

$$U(O(r), R(O(r))) < U(m_i, n \cdot k)$$

For simplicity, let $r = R(O(r))$, i.e., r is the last round in which the object $O(r)$ is selected. Thus,

$$U(O(r), r) < U(m_i, n \cdot k)$$

By line 6,

$$\forall m_i : U(O(r), r) \geq U(m_i, r)$$

Thus,

$$U(m_i, r) \leq U(O(r), r) < U(m_i, n \cdot k)$$

which is a contradiction to (10) since for some $r \leq n \cdot k - 1$, $U(m_i, r_1 = r) < U(m_i, r_2 = n \cdot k)$

Case 2: $m_i = O(n \cdot k)$. Consider round r' such that for all rounds $\{r' + 1, \ldots, n \cdot k\}$, object m_i is chosen. In this case, the R.H.S. of the equation (12) is $< U(m_i, r' + 1)$ since the utility only reduces with further inclusions of m_i. Following steps similar to Case 1 and considering a round r which is the last round for $O(r)$ to be selected,

$$U(O(r), r) < U(m_i, r' + 1)$$

By line 6,

$$\forall m_i : U(O(r), r) \geq U(m_i, r)$$

Thus,

$$U(m_i, r) \leq U(O(r), r) < U(m_i, r' + 1)$$

which is a contradiction to (10) since for some $r \leq r'$, $U(m_i, r_1 = r) < U(m_i, r_2 = r' + 1)$.

This proves that Algorithm 1 follows the constraint of Eq (5), and since by Lemma 5, Eq (5) implies (4), a correlated equilibrium is established.

□

Appendix F.
Example for Algorithm 1

This example demonstrates the operation of algorithm 1 with $n = 3$ parties, $m = 5$ objects, $k = 2$ size of inclusion list and $U = [8, 6, 5, 3, 1]$ utility values of the objects.

In Step 1, the algorithm iteratively selects the highest-value objects from U, dynamically adjusting selection counts in N. This process continues until $n \cdot k$ selections are made or all objects are fully allocated.

In Step 2, the algorithm distributes the selected objects among the players. The objects are allocated based on their adjusted utilities U_f and assigned in decreasing order of U_f. Each round assigns objects in order, updating the players' inclusion arrays L_i. Step 2 starts with $U = [8, 6, 5, 3, 1$, $N = [2, 2, 1, 1, 0]$, $U_f = [4, 3, 5, 3, 0]$, and $A = [2, 0, 1, 3, 4]$

Loop	U_{curr}	s	N	U after update
1	[8, 6, 5, 3, 1]	0	[1, 0, 0, 0, 0]	[8, 6, 5, 3, 1]
2	[4, 6, 5, 3, 1]	1	[1, 1, 0, 0, 0]	[8, 6, 5, 3, 1]
3	[4, 3, 5, 3, 1]	2	[1, 1, 1, 0, 0]	[8, 6, 5, 3, 1]
4	[4, 3, 2.5, 3, 1]	0	[2, 1, 1, 0, 0]	[8, 6, 5, 3, 1]
5	[2.66, 3, 2.5, 3, 1]	1	[2, 2, 1, 0, 0]	[8, 6, 5, 3, 1]
6	[2.66, 1.5, 2.5, 3, 1]	3	[2, 2, 1, 1, 0]	[8, 6, 5, 3, 1]

Round	Description	Variable State
1	Assign $A[0]$ once, $A[1]$ twice	L = [[0, 0, 1, 0, 0], [1, 0, 0, 0, 0], [1, 0, 0, 0, 0]]
2	Assign $A[2]$ twice, $A[3]$ once	L = [[0, 1, 1, 0, 0], [1, 1, 0, 0, 0], [1, 0, 0, 1, 0]]

Appendix G.
Details for analysis of Aggregation Phase

In this section, we will analyze the utility of IL proposers in the absence of adversarial censorship. In such a case, the proposer will select the highest bid amongst all the bids. The first thing to observe is that not all parties may have an incentive to broadcast, so let's assume that η (At equilibrium, $\gamma = \eta/n$) InpLs are publicly available. Consider that the IL proposer includes all the input lists it receives and its own. The IL proposer has two options: make its InpL available (**F** = 1) or withhold it (**F** = 0). If the IL proposer makes its input list available, then the following lemma holds.

Lemma 6. *Given an IL proposer P with a utility u_{il} for inclusion of its input list and u_{agg} for winning the auction for aggregation. Given η input lists are available (except its own), and the total number of IL proposers is n. Given P generates a bias $b \leq 1$. If P chooses to make its InpL available, its expected utility is $u_{il} + \mathsf{negl}(n)$.*

Proof. The bid generated by P is calculated as $\eta + 1 + b$. All other IL proposers also receive the input list of P. There exist two classes of other IL proposers: 1) those that made their input list available (there exist η such IL proposers) and those that did not $(n - \eta - 1)$. Let b_i represent the bias generated through VRF for IL proposer P_i.

The bid for each IL proposer who did not make its input list available is $\eta + 2 + b_i$ ($\eta + 1$ from publicly available lists, and 1 private). Similarly, the bid for each IL proposer who chose to make its input list available is $\eta + 1 + b_i$ (Its list is included in the publicly available lists).

The probability that P wins the auction is the same as the bid generated by P being greater than all other bids.

$$
\begin{aligned}
\mathbb{P}(P \text{ wins}) &= \prod_{i=0}^{\eta} \mathbb{P}(\eta + 1 + b \geq \eta + 1 + b_i) \\
&\quad \cdot \prod_{i=0}^{n-\eta-1} \mathbb{P}(\eta + 1 + b \geq \eta + 2 + b_i) \\
&= \prod_{i=0}^{\eta} \mathbb{P}(b \geq b_i) \cdot \prod_{i=0}^{n-\eta-1} \mathbb{P}(b \geq 1 + b_i) \\
&= \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \prod_{i=0}^{n-\eta-1} \{\mathbb{P}(b \leq 1)\mathbb{P}(b \geq 1 + b_i | b \leq 1) \\
&\qquad + \mathbb{P}(b > 1)\mathbb{P}(b \geq 1 + b_i | b > 1)\} \\
&= \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \prod_{i=0}^{n-\eta-1} (\mathbb{P}(b > 1)\mathbb{P}(b - 1 \geq b_i | b > 1))
\end{aligned}
\tag{13}
$$

If $b \leq 1$, the probability of winning the auction is 0, unless all parties ($\eta = n-1$) make their input lists available.

The utility in this case is given by u_{il}. If all parties make their list available, then the utility would increase by $(\frac{b}{b_{max}})^n \cdot u_{agg}$, which is negligible in n. □

Lemma 7. *Given an IL proposer P with a utility u_{il} for inclusion of its input list and u_{agg} for winning the auction for aggregation. Given η input lists are available (except its own), and the total number of IL proposers is n. Given P generates a bias $b > 1$. If the IL proposer chooses to make its InpL available, then its expected utility is $u_{il} + \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1} u_{agg}$*

Proof. From (13), the probability of winning the auction is

$$
\mathbb{P}(P \text{ wins}) = \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1}
$$

If P wins the auction, then it will receive both input list inclusion and aggregation rewards, while if it loses the auction, then the reward earned is only the input list inclusion reward.

$$
\begin{aligned}
u_P &= \mathbb{P}(P \text{ wins})(u_{agg} + u_{il}) + (1 - \mathbb{P}(P \text{ wins}))\, u_{il} \\
&= u_{il} + \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1} u_{agg}
\end{aligned}
\tag{14}
$$

□

Lemma 8. *Given an IL proposer P with a utility u_{il} for inclusion of its input list and u_{agg} for winning the auction for aggregation. Given η input lists are available (except its own), and the total number of IL proposers is n. Given P generates a bias $b < b_{max} - 1$. If the IL proposer chooses not to make its InpL available, then its expected utility is $\left(\frac{b+1}{b_{max}}\right)^{\eta} \cdot \left(\frac{b}{b_{max}}\right)^{n-\eta-1} (u_{agg} + u_{il})$*

Proof. The bid generated by P is $\eta + 1 + b$. All other IL proposers can not extend their bid with the input list of P. There exist two classes of other IL proposers - those that made their input lists available (there exist η such IL proposers) and those that did not $(n-\eta-1)$. Let b_i represent the bias generated through VRF for IL proposer P_i.

The bid for each IL proposer who made their input list available is $\eta + b_i$. Similarly, the bid for each IL proposer who did not is $\eta + 1 + b_i$.

The probability that P wins the auction is the same as the bid generated by P being greater than all other bids.

$$
\begin{aligned}
\mathbb{P}(P \text{ wins}) &= \prod_{i=0}^{\eta} \mathbb{P}(\eta + 1 + b \geq \eta + b_i) \\
&\quad \cdot \prod_{i=0}^{n-\eta-1} \mathbb{P}(\eta + 1 + b \geq \eta + 1 + b_i) \\
&= \prod_{i=0}^{\eta} \mathbb{P}(b + 1 \geq b_i) \cdot \prod_{i=0}^{n-\eta-1} \mathbb{P}(b \geq b_i)
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{P}(b + 1 \geq b_i) &= \mathbb{P}(b \leq b_{max} - 1)\mathbb{P}(b + 1 \geq b_i | b \leq b_{max} - 1) \\
&\quad + \mathbb{P}(b > b_{max} - 1)\mathbb{P}(b + 1 \geq b_i | b > b_{max} - 1)
\end{aligned}
$$

If $b > b_{max} - 1$, then $b + 1$ is always $> b_i$. Thus,

$$
\begin{aligned}
\mathbb{P}(b + 1 \geq b_i) &= \mathbb{P}(b \leq b_{max} - 1)\mathbb{P}(b + 1 \geq b_i | b \leq b_{max} - 1) \\
&\quad + \mathbb{P}(b > b_{max} - 1)
\end{aligned}
\tag{15}
$$

Since $b < b_{max} - 1$,

$$
\begin{aligned}
\mathbb{P}(b + 1 \geq b_i) &= \mathbb{P}(b + 1 \geq b_i | b \leq b_{max} - 1) \\
&= \left(\frac{b+1}{b_{max}}\right)
\end{aligned}
$$

Similarly,

$$
\mathbb{P}(b \geq b_i) = \frac{b}{b_{max}}
$$

Thus, given $b \leq b_{max} - 1$, the probability of winning the auction is

$$
\mathbb{P}(P \text{ wins}) = \left(\frac{b}{b_{max}}\right)^{n-\eta-1} \cdot \left(\frac{b+1}{b_{max}}\right)^{\eta}
$$

If P wins the auction, then it will receive both input list inclusion and aggregation rewards, while if it loses the auction, then no reward is earned since the input list was not available to others.

$$
\begin{aligned}
u_P &= \mathbb{P}(P \text{ wins})(u_{agg} + u_{il}) \\
&= \left(\frac{b+1}{b_{max}}\right)^{\eta} \cdot \left(\frac{b}{b_{max}}\right)^{n-\eta-1} (u_{agg} + u_{il})
\end{aligned}
$$

□

Lemma 9. *Given an IL proposer P with a utility u_{il} for inclusion of its input list and u_{agg} for winning the auction for aggregation. Given η input lists are available (except its* *own), and the total number of IL proposers is n. Given P generates a bias $b \geq b_{max} - 1$. If the IL proposer chooses not to make its InpL available, then its expected utility is $\left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il})$*

Proof. Equation (15) still holds for the analysis of this Lemma. Given $b > b_{max} - 1$, we get

$$\mathbb{P}(b + 1 \geq b_i) = 1$$

Thus,

$$\begin{aligned}
\mathbb{P}(P \text{ wins}) &= \left(\frac{b}{b_{max}}\right)^{n-\eta-1} \\
u_P &= \mathbb{P}(P \text{ wins})(u_{agg} + u_{il}) \\
&= \left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il})
\end{aligned}$$

□

Appendix H. Proofs for Section 5.2

Theorem 3. *Given an IL proposer P with a utility u_{il} for inclusion of its input list and u_{agg} for winning the auction for aggregation. Given η input lists are available (except its own), $b_{max} > 2$ and the total number of IL proposers is n.*

1) *Given P generates a bias $b \leq 1$. Except with a negligible probability, making its input list available is the dominant action for P.*
2) *Given P generates a bias $1 < b < b_{max} - 1$. Except with a negligible probability, making its input list available is the dominant action for P. Consequently (from parts 1 and 2 of the theorem), at least $\frac{b_{max}-1}{b_{max}}$ of the parties broadcast their input list in expectation.*
3) *Given P generates a bias $b \geq b_{max} - 1$. The Nash equilibrium for the game would be a mixed strategy, i.e., make its input list available with some probability and withhold with some probability.*

Proof. 1) From Lemma 6, the utility from making its input list available is u_{il}. From Lemma 8, the utility from making its input list available is

$$\left(\frac{b+1}{b_{max}}\right)^{\eta} \cdot \left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il})$$

Since $b_{max} > 2$ and $b \leq 1$, this utility tends to 0. Thus, the utility from making its input list available (u_{il}) is greater than that of not making its input list available (0). Thus, all such parties would make their input list available.

2) From Lemma 7, the utility from making its input list available is

$$u_{il} + \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1} u_{agg}$$

From Lemma 8, the utility of not making its input list available is

$$\left(\frac{b+1}{b_{max}}\right)^{\eta} \cdot \left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il})$$

Consider the difference between the utilities.

$$\begin{aligned}
&u_{il} + \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1} u_{agg} \\
&\quad - \left(\frac{b+1}{b_{max}}\right)^{\eta} \cdot \left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il}) \\
&\geq u_{il}\left(1 - \left(\frac{b+1}{b_{max}}\right)^{n-1}\right) \\
&\quad + u_{agg}\left(\left(\frac{b}{b_{max}}\right)^{n-1} - \left(\frac{b+1}{b_{max}}\right)^{n-1}\right) \\
&\geq u_{il}\left(1 - \left(\frac{b+1}{b_{max}}\right)^{n-1}\right) - u_{agg}\left(\frac{b+1}{b_{max}}\right)^{n-1} \\
&= u_{il}\left(1 - \left(1 + \frac{u_{agg}}{u_{il}}\right)\left(\frac{b+1}{b_{max}}\right)^{n-1}\right)
\end{aligned}$$

To ensure this is ≥ 0, we require

$$\left(\frac{b+1}{b_{max}}\right)^{n-1} < \frac{u_{il}}{u_{il} + u_{agg}}$$

The probability for this is given by

$$\mathbb{P} = \frac{b_{max}\left(\frac{u_{il}}{u_{il}+u_{agg}}\right)^{1/n\,-\,1} - 1}{b_{max} - 1}$$

which is approximately 1 if n is large. Thus, parties with $b < b_{max} - 1$ are incentivized to make their input list available. This occurs with a probability of $\frac{b_{max}-1}{b_{max}}$, which implies that in expectation, at least $\frac{b_{max}-1}{b_{max}} \cdot n$ parties would make their input lists available.

3) From Lemma 7, we know that the utility from making its input list available is

$$u_{il} + \left(\frac{b}{b_{max}}\right)^{\eta} \cdot \left(\frac{b-1}{b_{max}}\right)^{n-\eta-1} u_{agg}$$

From Lemma 9, the utility of not making its input list available is

$$\left(\frac{b}{b_{max}}\right)^{n-\eta-1}(u_{agg} + u_{il})$$

From Part 2, we know that η is in expectation more than $\frac{b_{max}-1}{b_{max}}n$. Substituting in Lemma 9, we get

$$\left(\frac{b}{b_{max}}\right)^{\frac{n}{b_{max}}-1}(u_{agg} + u_{il})$$

As b approaches b_{max}, the difference in utility is

$$u_{il} + 0 - \left(1 - \left(\frac{n}{b_{max}} - 1\right)\left(\frac{b_{max} - b}{b_{max}}\right)\right)(u_{agg} + u_{il})$$
$$= \left(\left(\frac{n}{b_{max}} - 1\right)\left(\frac{b_{max} - b}{b_{max}}\right)\right)(u_{agg} + u_{il}) - u_{agg}$$

which is negative since the first term approaches 0. Thus, at least some parties are incentivized not to make their input list available, and a mixed Nash equilibrium follows.

□

Appendix I. Details for Censorship Resistance in Input Building

However, we need to consider the expected number of broadcast input lists when considering the utility that the IL proposers receive from transactions. Let n_t be the number of input lists suggested to include the transaction ($n_t = |N_t|$), $\overline{n_t}$ as the expected number of broadcast input lists that contain the target transaction ($\overline{n_t} = n_t \cdot \gamma$, where γ is the probability that an IL proposer broadcasts), $\widetilde{n_t} = 1 + \gamma(n_t - 1)$ represents the denominator as specified in Eq (5) and $\widehat{n_t}$ represents the actual number of input lists that broadcast the transaction.

The expected utility for each IL proposer from including the target transaction is $\frac{u_{m_t}}{\widetilde{n_t}}$ and excluding it and adding another transaction m_s gives some utility $\frac{u_{m_s}}{\widetilde{n_s}+\gamma}$. If m_s is available in the global mempool, then $\frac{u_{m_s}}{\widetilde{n_s}+\gamma} \leq \frac{u_{m_t}}{\widetilde{n_t}}$, otherwise the cost u_{m_s} would be an additional cost to the adversary (and $n_s = 0$). Also, consider the utility for including the input list as suggested, but without the target transaction to be u_{il}^{-}, which is the sum of the utility that each transaction in the list provides. The strategies that each IL proposer follows, given it receives some bribe from the adversary, are shown in Lemma 10.

Lemma 10. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in absence of adversary, and a set N_t ($|N_t| = n_t$) of IL proposers who are suggested to include the target transaction m_t (i.e., $L_i = m_t \cup L_i^{-}$). Consider a bribe (br) from the adversary to IL proposers in the set N_t to censor the target transaction (action 2) and replace it with a replacement transaction m_s.*

- *i) If $br \leq \frac{u_{m_t}}{\widetilde{n_t}} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, the IL proposer would reject the bribe and propose the suggested input list.*
- *ii) If $\frac{u_{m_t}}{\widetilde{n_t}} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} < br < u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, the IL proposers would reject the bribe with some non-zero probability.*
- *iii) If $br \geq u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, the IL proposer would always accept the bribe and ignore the transaction.*

Proof. The utility received by following the equilibrium strategy (or rejecting the bribe) is $\mathbb{U}_r = u_{il}^{-} + \frac{u_{m_t}}{\widehat{n_t}}$, where $u_{il}^{-} = \mathbb{U}(L_i^{-}, \_)$ is the utility received from selecting list L_i^{-} and $\widehat{n_t} = \widetilde{n_t}$, if all IL proposers include the transactions as suggested. If some IL proposers accept the bribe and exclude the transaction from their input list, then $\widehat{n_t} < \widetilde{n_t}$. The utility received for accepting the bribe is $\mathbb{U}_a = u_{il}^{-} + \frac{u_{m_s}}{\widetilde{n_s}+\gamma} + br$. Thus, $\mathbb{U}_r - \mathbb{U}_a = \frac{u_{m_t}}{\widehat{n_t}} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} - br$. Since $1 \leq \widehat{n_t} \leq n_t$, we have that $\frac{u_{m_t}}{n_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} - br \leq \mathbb{U}_r - \mathbb{U}_a \leq u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} - br$. We now prove each part of the lemma separately.

- i) If $br \leq \frac{u_{m_t}}{\widetilde{n_t}} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, $\mathbb{U}_r - \mathbb{U}_a \geq 0$. Since the utility gained by the IL proposer from accepting the bribe is less than rejecting the bribe, the IL proposer would always reject the bribe.
- ii) If bribe $\frac{u_{m_t}}{\widetilde{n_t}} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} < br < u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, then the bribe is higher than the individual utility gained by the IL proposer if all other IL proposers choose to include the transaction (i.e., reject the bribe, $\widehat{n_t} = \widetilde{n_t}$). However, if all IL proposers choose to accept the bribe, then the utility received from rejecting the bribe and being the only IL proposer to include the target transaction is u_{m_t}. Thus, it is not rational for all IL proposers to accept or reject the bribe. A mixed Nash equilibrium would exist since both pure strategies are not an equilibrium, implying a non-zero probability of rejecting the bribe.
- iii) If $br \geq u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$, $\mathbb{U}_r - \mathbb{U}_a \leq 0$. Since the bribe available is greater than the utility that the IL proposer could receive, even if any other party does not include the transaction, the IL proposer always chooses to accept the bribe.

□

Lemma 11. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in the absence of an adversary, the adversary must pay at least $u_{m_t} \cdot (n_t - 1)$ to ensure (with probability = 1) that the target transaction does not appear in any input lists.*

Proof. From Lemma 10, if the adversary bribes the IL proposers in the set N_t in such a way that the IL proposers always censor the transaction, then the bribe has to be at least $u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma}$. Now, if m_s is a public transaction, i.e., available in mempool, then $u_{m_t} - \frac{u_{m_s}}{\widetilde{n_s}+\gamma} \geq u_{m_t} - \frac{u_{m_t}}{\widetilde{n_t}} \geq u_{m_t} - \frac{u_{m_t}}{n_t}$. Since at least n_t parties receive this bribe, the total cost to the adversary is at least $u_{m_t} \cdot (n_t - 1)$ to bribe all the IL proposers in set N_t. However, if the transaction is private, then the cost to the adversary is $u_{m_s} + br = u_{m_t}$. This amount must be given to all n_t parties, and thus the total cost would be $u_{m_t} n_t > u_{m_t} \cdot (n_t - 1)$ □

If the adversary chooses a strategy to bribe IL proposers to exclude the target transaction (Action 2), it must pay a cost of at least $u_{m_t} \cdot (n_t - 1)$ as shown in Lemma 11.

Consider Action 1. The adversary may choose to add spam transactions in such a way that the target transaction does not appear in any input list, or it may choose to reduce the number of n_t, and then follow up with Action 2.

Before we proceed with the analysis of this action, we need to observe the dependence of n_t on the fee paid by the transaction u_{m_t} and the fee paid by other transactions. Let $T(M)$ represent all the transactions the input list-building mechanism chooses. From Eq (5) for a correlated equilibrium, we know that,

$$\forall m_i \in T(M) : \frac{u_{m_i}}{\widetilde{n_i}} \geq \frac{u_{m_t}}{\widetilde{n_t} + \gamma}$$

Since $\widetilde{n_i} > 0$ for all $m_i \in T(M)$, we have

$$\forall m_i \in T(M) : u_{m_i}(\widetilde{n_t} + \gamma) \geq u_{m_t}\widetilde{n_i}$$

Taking the sum over all $m_i \in T(M)$, and noting that $\frac{u_{m_t}}{\widetilde{n_t}} > \frac{u_{m_t}}{\widetilde{n_t}+\gamma}$

$$\sum_{i \in T(M)} u_{m_i}(\widetilde{n_t} + \gamma) > u_{m_t} \sum_{i \in T(M)} \widetilde{n_i}$$

$$\sum_{i \in T(M)} u_{m_i}(\widetilde{n_t} + \gamma) > u_{m_t} \cdot n \cdot k \cdot \gamma$$

Let σ represent $\sum\limits_{i \in T(M)} u_{m_i}$. Also, $\widetilde{n_t} = 1 + \gamma(n_t - 1)$. Thus,

$$1 + \gamma n_t > \gamma \cdot n \cdot k \frac{u_{m_t}}{\sigma}$$

$$n_t > n \cdot k \frac{u_{m_t}}{\sigma} - \frac{1}{\gamma} \tag{16}$$

Using Action 1, the adversary can censor the target transaction by adding transactions to the mempool. If more transactions are to be chosen, then the algorithm would suggest the transaction to fewer parties. If we view these extra transactions as a sequential addition of transactions to the mempool, we will reach a point where the target transaction is suggested to only one IL proposer. In other words, the Lemma 12 compares using Action 1 to censor completely and a hybrid of Action 1 and Action 2 to first reduce the number of IL proposers and then bribe the rest. The lemma prooves that the latter is a dominant action.

Lemma 12. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in absence of adversary, if the adversary reduces the number of times the transaction is suggested to $n_t = 1$ (Action 1), then after reaching this state, the cost incurred to an adversary in bribing the IL proposer (Action 2) is lower than adding further transactions to reduce the number of parties that are suggested to include the transaction (Action 1).*

Proof. To displace the target transaction, the adversary would have to displace all selections of the transactions after the target transaction is chosen for the first time in Algorithm 1 since each of the transactions that are selected after the target transaction gave lower utility than the first selection of the target transaction. Thus, in the worst case for $n_t = 1$, the target transaction is the last transaction chosen in Step 1 of Algorithm 1 such that there are no other transactions to displace. To displace the last chosen object (which in this case is m_t), the adversary would need to add a transaction m_a such that $\frac{u_{m_a}}{\widetilde{n_a}+\gamma} \geq \frac{u_{m_t}}{\widetilde{n_t}}$. Since $n_t = 1$, $\widetilde{n_t} = 1$, this implies $u_{m_a} \geq u_{m_t}$. Thus, Action 1 costs at least u_{m_t}.

If the adversary instead chooses to bribe the IL proposer, then from Lemma 10 the minimum bribe it would have to pay the IL proposers is $u_{m_t} - u_{m_s} \leq u_{m_t} \leq u_{m_a}$, where u_{m_s} represents the utility of some replacement transaction that the IL proposer could include. Thus, Action 2 costs at most u_{m_t}.

Thus, bribing the IL proposer dominates the action of displacing the transaction through added adversarial transactions when the target transaction appears only once. □

Lemma 13. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in absence of adversary, if the adversary adds adversarial transactions (Action 1) with a total fee of u_{m_a} and pays a bribe br_1 to all the IL proposers which are suggested to add the target transaction (Action 2). If $u_{m_t} \leq \frac{\sigma}{\sqrt{nk}}$, then the cost incurred by the adversary is greater than $u_{m_t}(n \cdot k \frac{u_{m_t}}{\sigma} - 1 - \gamma)$*

Proof. If the adversary does not add any adversarial transaction, then the cost to the adversary by only bribing is given from Lemma 11 and Eq.(16). This cost is represented by

$$C = u_{m_t}(n \cdot k \frac{u_{m_t}}{\sigma} - 1 - \frac{1}{\gamma})$$

Since no additional transactions are added, the cost to the adversary is only the bribe. Thus, $br_1 + u_{m_a} \geq C$ in this case.

If the adversary adds some transactions to reduce the number of times the target transaction appears in algorithm 1, and then censors the rest (hybrid of action 1 and action 2) then the cost to the adversary is given by the fees paid plus the bribe cost to remove the target transaction from the reduced number of input lists.

$$C_1 = u_{m_a} + br_1$$

From Lemma 11 and Eq.(16), we have

$$\begin{aligned} br_1 &\geq u_{m_t}({n_t}' - 1) \\ {n_t}' &\geq n \cdot k \cdot \frac{u_{m_t}}{\sigma - \sum(u_l) + u_{m_a}} - \frac{1}{\gamma} \\ &\geq n \cdot k \cdot \frac{u_{m_t}}{\sigma + u_{m_a}} - \frac{1}{\gamma} \end{aligned}$$

, where $\sum(u_l)$ represents the sum of any transactions removed. Thus,

$$C_1 \geq u_{m_a} + u_{m_t}(n \cdot k \cdot \frac{u_{m_t}}{\sigma + u_{m_a}} - 1 - \frac{1}{\gamma})$$

The difference in this cost to the adversary and the minimum cost we claim is given by

$$\begin{aligned} C_1 - C &\geq u_{m_a} - u_{m_t}(nku_{m_t}) \cdot \left(\frac{1}{\sigma} - \frac{1}{\sigma + u_{m_a}}\right) \\ &\geq u_{m_a} - nku_{m_t}^2 \left(\frac{u_{m_a}}{\sigma(\sigma + u_{m_a})}\right) \end{aligned}$$

If $u_{m_t} \leq \frac{\sigma}{\sqrt{nk}}$, then $u_{m_t}^2 \leq \frac{\sigma^2}{nk}$. Thus,

$$C_1 - C \geq u_{m_a} - \sigma^2 \left(\frac{u_{m_a}}{\sigma(\sigma + u_{m_a})}\right) \geq 0$$

Thus, $C_1 \geq C$ and the minimum cost that the adversary must pay is $u_{m_t}(n \cdot k\frac{u_{m_t}}{\sigma} - 1 - \frac{1}{\gamma})$. □

Appendix J. Details for Censorship Resistance in Aggregation

The first thing to note here is that the adversary can infer from Theorem 3 that if a proposer has not made its input list available, then the bias for such a party must be larger than one less than the maximum bias, i.e., $b > b_{max} - 1$. However, it cannot tell that if an IL proposer made its input list available that the bias for the party is $\leq b_{max} - 1$, since an IL proposer may still choose to make its input list available even if the bias for it is $> b_{max} - 1$ (since it is a mixed Nash equilibrium). Next, we also note that Action 4 cannot censor the target transaction since, under honest conditions, each bid would contain all input lists, including those containing the target transaction; excluding θ of them would not censor the target. Thus, we would look at Action 4 as a sub-routine within Action 3.

Lemma 14. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in absence of adversary, given $\widehat{n_t}$ is the number of input lists that contain the target transaction, m_t. Given an IL proposer P which generates a bias $b \geq b_{max} - \widehat{n_t}$. If $br < u_{agg}/2$, then P would reject the bribe with some non-zero probability. If $br \geq u_{agg}/2$, then P would accept the bribe.*

Proof. In order to remove the target transaction m_t, the adversary requires the IL proposers to exclude all $\widehat{n_t}$ input lists that contain it. This would reduce the bid the IL proposer can send by $\widehat{n_t}$. Let's consider the case where $br \leq u_{agg}/2$. At equilibrium, let the probability with which the bribe is rejected be p.Consider the case of $p = 0$. If all IL proposers decide to accept the bribe, then if P rejects the bribe, the adversary would drop its bid amongst the θ crash faults tolerated. However, in subsequent blocks, this bid would be included with proof that the bid was higher than the winning bid. (There is no incentive for the adversary to censor it in later rounds). This yields a utility of $u_{agg}/2$ for P. Thus, the incentive from rejecting the bribe is at least $u_{agg}/2$. If the bribe is less than $u_{agg}/2$, then all parties would have an incentive to reject the bribe with some non-zero probability.

For the case that $br \geq u_{agg}/2$, if the IL proposer rejects the bribe, the maximum utility it can get is by winning the highest bid reward of $u_{agg}/2$ (while it would also have to pay a fee to get its bid included in the later round). Thus, it would always accept the bribe if $br \geq u_{agg}/2$. □

As a consequence of Lemma 14, if the bribe offered is $< u_{agg}/2$, then the number of bids submitted by IL proposers that do not accept bribes is (with some probability) greater than θ. Thus, the bribery fails with some probability.

Lemma 15. *Given all IL proposers follow strategy Ψ as described in Algorithm 1 in absence of adversary, given $\widehat{n_t}$ is the number of input lists that contain the target transaction, and η is the total number of input lists available. If an adversary wants to censor the target transaction (with 100% probability) by bribing during the aggregation phase, then the total cost incurred by the adversary is at least $(n - \theta) \cdot u_{agg}/2$.*

Proof. From Lemma 14, the minimum bribe required to bribe an IL proposer who draws a bias $> b_{max} - \widehat{n_t}$ would be $u_{agg}/2$. However, the adversary does not know which parties draw such a bias. The adversary can identify that each IL proposer that did not broadcast the input list would have (with a high probability) a bias greater than $b_{max} - 1$; however, this does not give any information about an IL proposer drawing a bias less than $b_{max} - n_t$. This implies that the adversary would have to bribe all but θ IL proposers regardless of the value of bias drawn. Thus, the total bribe the adversary has to pay is $(n - \theta) \cdot u_{agg}/2$. □

From Lemma 15, we observe that any bribery for parties in the aggregation phase (hybrids of Actions 3 and 4 is independent of the number of times the target transaction appears in the input lists. Thus, a reduction of the number of times the target transaction appears in input lists by Actions 1 and 2 has no reduction in the cost to an adversary when it takes Actions 3 and 4. Thus, the two sets of actions are independent.

Appendix K. Proof for Theorem 6

Theorem 6. *Given n parties running the protocol, M represents the transactions available to all parties in the mempool, f_j represents the fee paid by a transaction $m_j \in M$, $\theta - 1$ represent the number of crash faults tolerated, and T represent the union of all lists L_j when Algorithm 1 is run on M. Consider $B = \{br_1, \ldots, br_{|T(M)|}\}$ such that $br_j = \min((n \cdot k\frac{f_j}{\sigma} - 1 - \frac{1}{\gamma})f_j, \frac{(n-\theta)}{\sqrt{n}}\sigma, R)$. The protocol satisfies (B, θ, T)-censorship resistance.*

Proof. Consider an adversary with a bribery budget of br. From Lemma 13, we know that if the adversary attempts to censor a transaction m_j from the input list, the least amount of bribe it must pay is

$$(n \cdot k\frac{f_j}{\sigma} - 1 - \frac{1}{\gamma})f_j$$

Note that here, $k \cdot f_j < \sigma$ and $f_j \leq \frac{\sigma}{\sqrt{nk}}$. If the adversary attempts to censor the transaction in the aggregation phase, then the total cost, as governed by Lemma 15 is

$$(n - \theta)u_{agg} = (n - \theta)\sqrt{n}u_{il} \geq (n - \theta)\sqrt{n}\sigma/n$$
$$\geq \frac{(n - \theta)}{\sqrt{n}}\sigma$$

Now, let $br_i = \max((n \cdot k\frac{f_j}{\sigma} - 1 - \frac{1}{\gamma})f_j, \frac{(n-\theta)}{\sqrt{n}}\sigma, R)$.

If $br < br_i$, then at least θ parties will output the inclusion list, which includes the transaction m_i, implying that the proposer will select the inclusion list with transaction m_i at least once. Thus, the protocol is (B, θ, T)–censorship resistant. □