EPBS DESIGN DOC

MALLESH PAI[A] AND MAX RESNICK[B]

Enshrined PBS (herein, ePBS) aims to move the current PBS system on-chain, reducing the underlying trust assumptions (in particular, the trusted relay) and therefore have a more credibly neutral/ decentralized system. Neuder and Drake (2023) list several desiderata that we recount below, which they posit that an ePBS solution should satisfy.

One of the properties that they list is *censorship resistance* (CR). Our point of departure is that CR is an important property, not just for the blockchain but also for faithfully executing the PBS auction on-chain (Pai et al., 2023). To illustrate why, we consider the Two Block Head Lock (TBHL) proposal of Neuder and Drake (2023) described in Figure 1 and consider how it interacts with MEV Burn (Drake, 2023).[1]

PROCEDURE 1. Two Block Head Lock (Neuder and Drake, 2023)

(1) Builders submit bids for blocks, by announcing a block header and the bid, i.e., the amount they will pay the proposer.
(2) The proposer selects a winning bid, and announces the first block containing solely their commitment to this bid, i.e., the signed header corresponding to this bid.
(3) The attesting committee locks onto the first block containing the signed header.
(4) The winning builder checks for equivocation in the first stage and then announces their block, and this is then proposed by the proposer.
(5) Validators check that the announced block 2 corresponds to the block header committed to in block 1.

[A]DEPARTMENT OF ECONOMICS, RICE UNIVERSITY AND SPECIAL MECHANISMS GROUP MALLESH.PAI@SPECIALMECHANISMS.ORG
[B] SPECIAL MECHANSISMS GROUP MAX@SPECIALMECHANISMS.ORG
Date: June 2023.
[1]MEVBurn Proposes to take the revenue from the ePBS auction and burn it rather than transferring it to the proposer.

To understand the issue, consider the proposer's incentives in Step 2. In a setting where the proposer keeps the bid, their incentives are *aligned* with efficiency, i.e. they are incentivized to select the highest bid.

However, suppose that MEVburn is implemented. In this case the amount of the selected (winning) bid is burned rather than paid to the proposer. Note that now the validator has no incentive to select the highest bid in step 2: they are indifferent across all bids and a bidder could, for example, side contract (bribe) the proposer to be selected despite not having the highest bid. Note that TBHL contains no protection against such behavior, indeed, such if all other bidders are bidding "honestly" the deviation described above is profitable for the deviating bidder and the proposer. Even if the validator receives a portion of the bid and the remainder is burned, such side contracts may still be profitable for the proposer.

As a result, to ensure that the auction results in the correct outcome, it is necessary that not just the the winning bid, but all bids, are included on chain in step 2, so that validators can attest to the fact that the "correct" winner was selected. Requiring all bids to be reported on chain, however does not solve the problem. Essentially, every valid bid for ePBS auction is now a transaction to be included in the block: but inclusion is determined by the proposer! This problem was studied in Pai et al. (2023), who showed that single-block auctions have poor outcomes when conducted on a block chain that is not censorship resistant.

1. Censorship Resistance: A Definition and a Solution (Pai et al., 2023)

The following is based on Pai et al. (2023) and provides a formal definition of censorship resistance: we abstract away from the details of the blockchain and instead consider solely the functionality as a public bulletin board. The public bulletin board can be written to, which is how bids may be submitted, and can be read from, which is how the PBS auction can then be executed. For simplicity, we assume that once a message has been successfully written the the bulletin, it can be read without friction. For example, any transaction included in an Ethereum block can be read by any full node.

Definition 1 (Public Bulletin Board)**.** *A Public Bulletin Board has two publicly callable functions:*

(1) Write(m, t) *takes as input a message* m *and an inclusion tip* t *and returns* 1 *if the message is successfully written to the bulletin board and* 0 *otherwise.*

(2) Read() *returns a list of all messages that have been written to the bulletin board over the period.*

Some subtlety must be observed in the definition of a public bulletin board. First, the Write function takes as input not only a message m but also a tip t. Here our definition departs from Choudhuri et al. (2017). This models proposer tips and other forms of validator bribes. To motivate this, consider that the write function on Ethereum is unlikely to succeed without a sufficient tip, and so the behavior of Write is very different depending on the size of the associated tip.

Example 1 (Single Block)**.** In the case of a single block, the Write(m, t) operation consists of submitting a transaction m with associated tip t. Write(m, t) succeeds if the transaction is included in that block on the canonical chain.

Example 2 (Multiple Blocks)**.** In the case of k blocks with rotating proposers, the $writeop(m, t)$ operation consists of submitting a transaction m with associated tip t during the period before the first block is formed. Write(m, t) succeeds if the transaction is included in any of the k blocks.

We can now model the relationship between the tip t and the success of the write operation as a function. This function provides a flexible definition of the bulletin board's censorship resistance.

DEFINITION 2 (Censorship Resistance of a Public Bulletin Board)**.** *The censorship resistance of a public bulletin board $\mathcal{D}$ is a mapping $\varphi : \mathbb{R}_+ \to \mathbb{R}_+$ that takes as input the tip t corresponding to the tip in the write operation* Write$(\cdot, t)$ *and outputs the minimum cost that a motivated adversary would have to pay to make the* Write *fail.*

This definition allows us to compare the censorship resistance of two bulletin boards even when the inner machinations of those are profoundly different. This definition also easily extends to cases where tips are multi-dimensional. i.e. $t \in \mathbb{R}_+^n$ by substituting $\varphi : \mathbb{R}_+ \to \mathbb{R}_+$ to $\varphi : \mathbb{R}_+^n \to \mathbb{R}_+$.

Example 3 (continues=ex:single)**.** The cost to censor this transaction would simply be t in the uncongested case because the motivated adversary has to compensate the proposer at least as much as the proposer would be losing from the tip. So:

$$\varphi(t) = t \tag{1}$$

Example 4 (continues=ex:multiple)**.** In the case of k blocks with rotating proposers, the Write(m, t) operation consists of submitting a transaction m with associated tip

t during the period before the first block is formed. Write(m, t) succeeds if the transaction is included in any of the k blocks. The cost to censor this transaction would be kt since each of the k proposers must be bribed at least t to compensate them for the forgone tip on the transaction that they each had the opportunity to include. So:

$$\varphi(t) = kt. \tag{2}$$

1.1. *Multiple Concurrent Block Proposers*

Depending on the number of bidders and the time constraints inherent to the specific auction application, it may not be feasible to hold the auction for long enough to achieve the desired censorship resistance level. For example for ePBS, time is critical (since we need to collect bids for the next block). To this end, we now consider k concurrent block proposers .

In view of the concurrency, we allow bidders to submit conditional tips, which depend on the number of proposers who include the transaction. For simplicity, we consider a *twin tip*, i.e., each bidder submits a conditional tip of the form (t, T), where T is paid if only a single proposer includes bidder 1's transaction and t is paid if more than one proposer includes the transaction.

OBSERVATION 1. *With k concurrent proposers and conditional tipping, the censorship resistance of a conditional tip (t, T) is straightforwardly verified as:*

$$\varphi(t, T) = kT. \tag{3}$$

It is important to note that the conditional tip disentangles the cost of inclusion (for the transacting party) from the cost of censoring, i.e. if $T \gg t$, then the censorship resistance is kT which is much larger than the cost of inclusion, kt.

2. Censorship Resistant ePBS

We are now in a position to describe an ePBS proposal that uses a censorship resistant bulletin board as a building block to produce the desired outcome. For instance, Multiple Concurrent Block Proposers with conditional tip logic, as described above, is strongly censorship resistant and can be used to implement the censorship resistant bulletin board.

PROCEDURE 2. Censorship Resistant ePBS

(1) Builders each submit (block-header, bid) to a censorship resistant bulletin board.
(2) The winning builder is the largest of the list of bids on the bulletin board.
(3) The winning builder announces their block.
(4) Validators check that the announced block 2 corresponds to the winning block header committed to in Step 1.

The bulletin board allows all builders to submit their bids in a censorship resistant way, such that the existence of these bids can be forensically verified on-chain. Attestors/ validators can therefore easily verify which bidder is the winner, and attest to only the corresponding block. As a result a separate proposer is not needed to announce the selected block: with an honest majority of attestors the winning builder can directly announce their block and have it attested to without fear of getting griefed etc.

3. Censorship Resistant Distributed Block Building

Finally, we outline a potential endgame that a censorship resistant bulletin boards could enable for ePBS which checks a lot of the boxes outlined in the forward compatibility desiderata of Neuder and Drake (2023), most importantly, distributed block building and compatibility with MEV burn.

We now describe the knapsack problem referenced in Procedure 3. A transaction t for our purposes consists of two parts, the transaction message m which contains execution logic and a bid b.

DEFINITION 3 (Progress)**.** *The* Progress(m, α) *function takes as input a precursor state* α *and execution logic* m *and returns the progressed state* α' *if it succeeds, otherwise*

PROCEDURE 3. Censorship Resistant Distributed Block Building

(1) Everyone submits their transactions of the form (m, b) to the censorship resistant bulletin board where m is a message and b is their bid for inclusion in the eventual execution block.
(2) The builders compute solutions to the block packing knapsack problem OPT based on the available transactions.
(3) Builders submit their knapsack solutions to the Censorship resistant inclusion layer.
(4) The best solution is self evident and is the canonical block.

it returns 0*, indicating that the transaction failed. If called on a precursor state of* 0*,* $\text{Progress}(m, 0)$ *returns* 0 *regardless of the message* m*.*

Let T be the set of all available transactions then define the set of possible blocks as

$$\mathcal{T} := \{\text{ordered finite sequences } t_1, \ldots, t_n | t_1, \ldots, t_n \in T\}$$

Then define the success function $S : \mathcal{T} \to \{0, 1\}$ where for any $\tau \in \mathcal{T}$, $S(\tau)$ is defined as:

$$S(\tau) = \begin{cases} 1 & \text{Progress}(m_n, \text{Progress}(m_{n-1}, \ldots \text{Progress}(m_1, \alpha_0))) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The packing/ building knapsack problem can now be written as:

$$\begin{aligned} &\text{maximize} && \sum_{i=1}^{n} b_i && \text{(OPT)} \\ &\text{subject to} && b_i \text{ are bids associated with } t_1, \ldots, t_n \in \mathcal{T} \\ & && S(t_1, \ldots, t_n) = 1. \end{aligned}$$

3.1. *Compatibility with MEV burn*

Note that the optimization problem outlined in OPT is computationally hard: formally, it is a bin packing problem with a collection of additional constraints defined by the success function S. Therefore, burning the entire value of the bids for inclusion to the winning block would be self-defeating since there would no incentives for block builders to invest resources into solving the difficult knapsack

problem. Instead, to optimize the incentives for block builders to invest in solving the knapsack problem, we propose to burn the amount of the second best solution submitted and the difference between the best solution and the second best solution goes to the builder who submitted the best block. The idea that giving the winning agent their *marginal contribution* to welfare aligns the incentive to invest is well studied, see e.g., Vickrey (1961), Krähmer and Strausz (2007) or Akbarpour et al. (2021).

4. Discussion

4.1. *Gossiping Bids*

An alternative to including bids on a censorship resistant bulletin board is to simply let these be gossiped. From an engineering perspective, this solution is simpler than a censorship resistant bulletin board. However formally, such attestation logic (requiring attestors to attest the validity of a proposed block based on off-chain considerations) violates forensic support and therefore is undesirable (Sheng et al., 2022). More speculatively, it is potentially another example of "overloading consensus," something that may not be desirable (see, e.g., Buterin (2023)).

4.2. *Light Clients*

One of the future compatibility desiderata was compatibility with stateless clients. Censorship resistant inclusion layers are compatible with proofs of inclusion that light clients are based on. This would allow a light client to verify that a bid or transaction was included on the public bulletin board without requiring them to know everything on the bulletin board.

4.3. *Garbage Collection*

One concern of censorship resistant bulletin boards is that the history of the bulletin board might contribute to state bloat Buterin (2020). After finalization takes place, full nodes could garbage collect transactions that were not included in blocks to reduce state bloat.

REFERENCES

Akbarpour, Mohammad, Scott Duke Kominers, Shengwu Li, and Paul R Milgrom, "Investment Incentives in Near-Optimal Mechanisms," in "Proceedings of the 22nd ACM Conference on Economics and Computation" 2021, pp. 26–26.

Buterin, Vitalik, "PBS Censorship Resistance," 2020.

_____, "Don't overload Ethereum's consensus," 2023.

Choudhuri, Arka Rai, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers, "Fairness in an Unfair World: Fair Multiparty Computation from public Bulletin Boards," Cryptology ePrint Archive, Paper 2017/1091 2017. https://eprint.iacr.org/2017/1091.

Drake, Justin, "MEV burn—a simple design," May 2023.

Krähmer, Daniel and Roland Strausz, "VCG mechanisms and efficient ex ante investments with externalities," *Economics Letters*, 2007, *94* (2), 192–196.

Neuder, Mike and Justin Drake, "Why enshrine Proposer-Builder Separation? A viable path to ePBS," May 2023.

Pai, Mallesh, Max Resnick, and Elijah Fox, "Censorship Resistance in On-Chain Auctions," 2023.

Sheng, Peiyao, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath, "Player-Replaceability and Forensic Support are Two Sides of the Same (Crypto) Coin," *Cryptology ePrint Archive*, 2022.

Vickrey, William, "Counterspeculation, auctions, and competitive sealed tenders," *The Journal of finance*, 1961, *16* (1), 8–37.