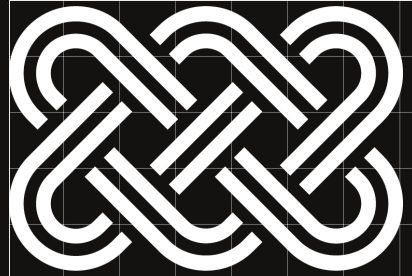
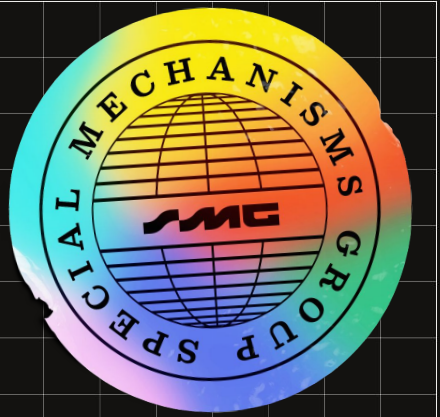




BRAID

Implementing Multiple Concurrent Proposers

Max Resnick

consensys

SMG

This is early stage work.

This is joint work with Mallesh Pai, Alberto Sonnino, Joachim Neu, and Joe Bonneau

]

Towards a Definition of Censorship Resistance

Definition (Public Bulletin Board)
A Public Bulletin Board has two public 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.

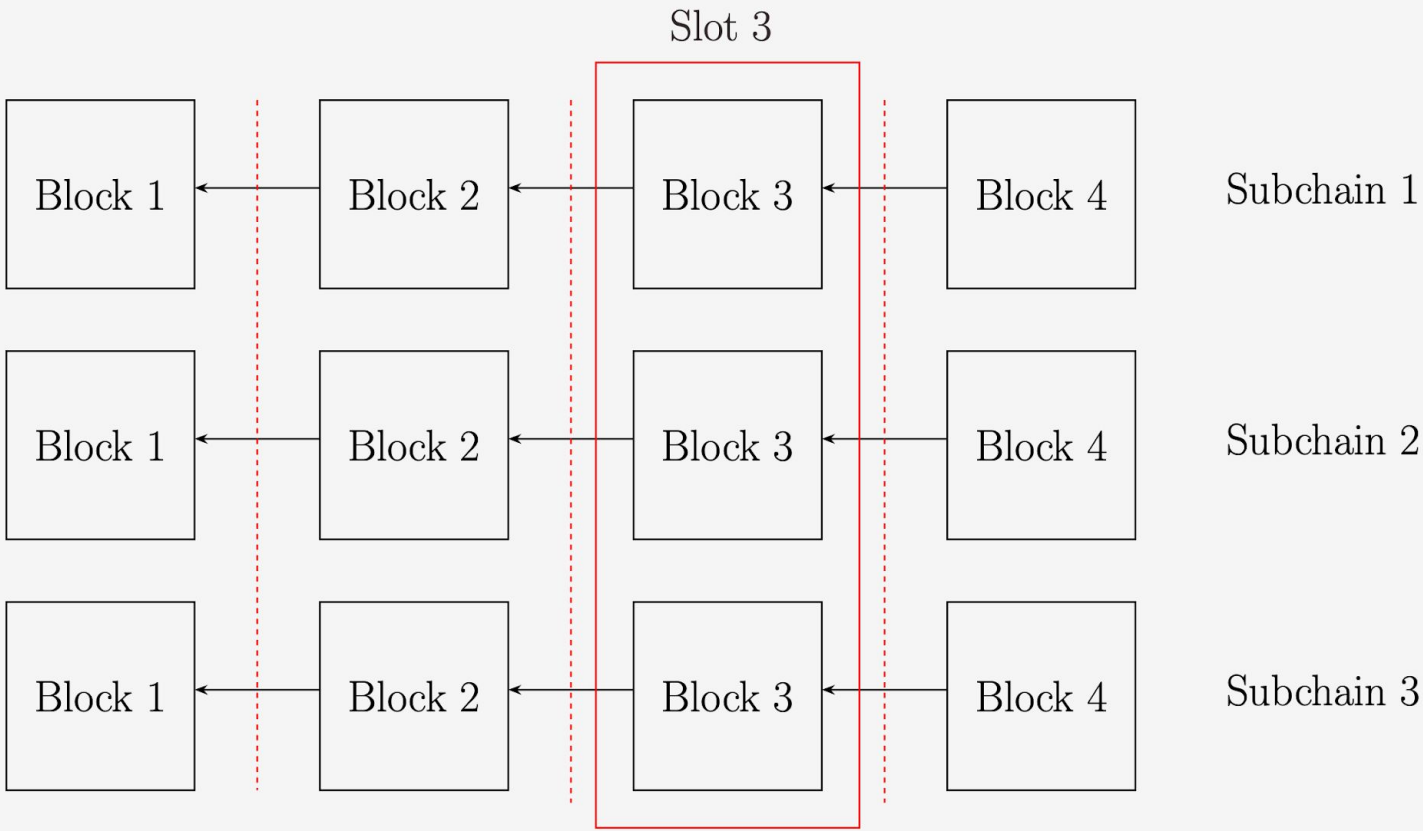
2. read() returns a list of all messages that have been written to the bulletin board over the period.

An Economic Definition of Censorship Resistance

Definition (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.

Theorem (Fox-Pai-Resnick 23)
With k concurrent proposers and conditional tipping, the censorship resistance of a conditional tip $(t,\ T)$ is $\varphi(t,\ T) = kT$.

Intuition: With multiple proposers competing to get a transaction on-chain, can set up a prisoner's dilemma among them. Expensive to censor, cheap to include.


Slot 3
Block 1
Block 2
Block 3
Block 4
Subchain 1
Block 1
Block 2
Block 3
Block 4
Subchain 2
Block 1
Block 2
Block 3
Block 4
Subchain 3