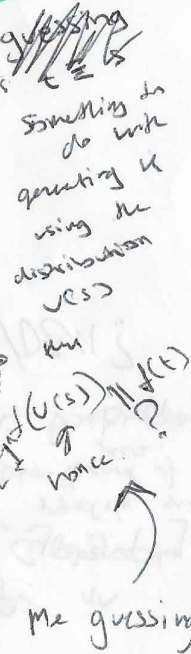


Simple protocol



We note that, while the blockchain address protocol is not part of the burn protocol, the security properties of a burn protocol Π will be defined with respect to a blockchain address protocol Π_α .

2 Defining Proof-of-Burn

We now formally define what a proof-of-burn protocol is. Let κ be the security parameter. The protocol consists of two functions `GenBurnAddr` and `BurnVerify` and works as follows. Alice first generates an address `burnAddr` to which she sends some cryptocurrency. The address is generated by invoking `GenBurnAddr($1^\kappa, t$)` and encodes information contained in a tag t ,

Potential malicious use:
Similar to scams where people get them to send their crypto, by reducing the

Constraints
Commits only to
a single
tag?

↓
you CANNOT
STOP MORONS!!

$S := \{s_1, \dots, s_n\} \mid n \in \mathbb{N}$
 (obviously not a monomorphism!)
 $d(S) := \frac{1}{|S|}$
 $[n] = \{1, \dots, n\}$ or $\mathbb{N}^?$
 $\mathbb{C}^n = \mathbb{C}^{(n)}$

As $|ADA| \rightarrow 1 \Rightarrow V(ADA) \rightarrow (V(ADA) + x)$
 $V(x)$ is vsd value.