

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 $\text{GenBurnAddr}(1^\kappa, t)$ and encodes information contained in a tag t ,