A Blockchain Execution We consider the execution of a blockchain protocol $(\Pi, \mathsf{extract})$ that is directed by an environment $Z(1^\kappa)$ (where κ is a security parameter), which activates a number of parties $1, 2, \ldots, n$ as either "honest" or corrupted parties. Honest parties execute Π on input 1^κ with an empy local state *chain*; corrupt parties are controlled by an attacker A which reads all their inputs/message and sets their outputs/messages to be sent.