A blockchain protocol is a pair of algorithms $(\Pi, \mathsf{extract})$ where Π is a stateful algorithm that receives a security parameter κ as inputs and maintains a local state *chain*. The algorithm $\mathsf{extract}(\kappa, chain)$ outputs an *ordered* sequence of "records", or "batches", $\vec{\mathsf{m}}$ (e.g., in the bitcoin protocol, each such record is an ordered sequence of transactions). We call $\mathsf{extract}(\kappa, chain)$ the "record chain" of a player with security parameter κ and local variable *chain*; to simplify notation, whenever κ is clear from context we often write $\mathsf{extract}(chain)$ to denote $\mathsf{extract}(\kappa, chain)$.