CommitCoin: Commitments with Temporal Dispute Resolution using Bitcoin
(A short paper)

September 15th, 2011

Jeremy Clark[1] and Aleks Essex[2]

[1] Carleton University
clark@scs.carleton.ca
[2] University of Waterloo
aessex@cs.uwaterloo.ca

Abstract. In the standard definition of a commitment scheme, the sender commits to a message and immediately sends the commitment to the recipient interested in it. However in a number of scenarios, the sender does not know who will become interested in the commitment at commitment time. Further, when the interested party does emerge, it could be critical to establish at what time the commitment was made. In this paper, we demonstrate how proof of work protocols can provide (fuzzy) verifiable timestamps for commitments without requiring a broadcast channel or any trusted/distributed third parties. We produce a threat model and note some limitations. We also present CommitCoin, an instantiation of the general approach that offloads the processing to the Bitcoin peer-to-peer network; a network used to mint and trade digital cash.