Cryptology ePrint Archive: Report 2011/677

CommitCoin: Carbon Dating Commitments with Bitcoin

Jeremy Clark and Aleksander Essex

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 the sender may not always know at the time of commitment who will become interested in verifying it. Further, when the interested party does emerge, it could be critical to establish when the commitment was made. Employing a proof of work protocol at commitment time will later allow anyone to "carbon date" when the commitment was made, approximately, without trusting any external parties. We present CommitCoin, an instantiation of this approach that harnesses the existing processing power of the Bitcoin peer-to-peer network; a network used to mint and trade digital cash.

Category / Keywords: applications / electronic commerce and payment, bit commitment

Publication Info: Full version of paper appearing at Financial Cryptography 2012.

Date: received 14 Dec 2011

Contact author: clark at scs carleton ca