OP_RETURN

From Bitcoin Wiki

OP_RETURN is a script opcode used to mark a transaction output as invalid. Since any outputs with OP_RETURN are provably unspendable, OP_RETURN outputs can be used to burn bitcoins.

Is storing data in the blockchain acceptable?

Many members of the Bitcoin community believe that use of OP_RETURN is irresponsible in part because Bitcoin was intended to provide a record for financial transactions, not a record for arbitrary data. Additionally, it is trivially obvious that the demand for external, massively-replicated data store is essentially infinite. Despite this, OP_RETURN has the advantage of not creating bogus UTXO entries, compared to some other ways of storing data in the blockchain.

From Bitcoin Core release 0.9.0 (https://bitcoin.org/en/release/v0.9.0#opreturn-and-data-in-the-block-chain):

This change is not an endorsement of storing data in the blockchain. The OP_RETURN change creates a provably-prunable output, to avoid data storage schemes – some of which were already deployed – that were storing arbitrary data such as images as forever-unspendable TX outputs, bloating bitcoin's UTXO database.

Storing arbitrary data in the blockchain is still a bad idea; it is less costly and far more efficient to store non-currency data elsewhere.

OP_RETURN applications

OP_RETURN can be used for digital asset proof-of-ownership, and has at times been used to convey additional information needed to send transactions (see stealth address).

OP_RETURN prefixes

Often, OP_RETURN transactions include a prefix to identify which "protocol" they belong to. Protocols wishing to claim OP_RETURN prefixes should use the standard Bitcoin Improvement Proposals process. Not all OP_RETURN transactions use prefixes.

https://en.bitcoin.it/wiki/OP_RETURN

- This page was last modified on 7 May 2017, at 02:17.
 Content is available under Creative Commons Attribution 3.0 unless otherwise noted.