Proof-of-HODL

Assessing HODLer sentiment using time-locked contracts

Tel Aviv Bitcoin emBassy 2017 Hackathon

Nadav Ivgi, Bitrated
nadav@bitrated.com

Bitcoin time scripting

- Bitcoin scripting can now use the time dimension!
- Enabled by CSV & relative time-lock (BIP 68 & 112)
  aka “what everyone thought nLocktime does until they took a closer look”, soft-forked into Bitcoin in July 2016
- Allows time-locking *outputs* for a predetermined amount of time or blocks (absolutely or relatively)
- Time-lock enforced by the Bitcoin network

Handicap principle

The handicap principle explains how evolution may lead to "honest" or reliable signaling between animals which have an obvious motivation to bluff or deceive each other.

The handicap principle suggests that reliable signals must be costly to the signaler, costing the signaler something that could not be afforded by an individual with less of a particular trait.

(From Wikipedia, the free encyclopedia)

Proof of HODL

Provably time-locking bitcoins as a cost-function for reliable signaling

Bitcoins x Time locked = *Bitcoin Days Locked*

- Build trust for online identities
- Anti-spam measure
- HODL-weighted voting

HODL-weighted voting

Giving HODLers a voice

- Provably HODLing shows vested interest (takes away the ability to sell)
- The more you're willing to go long, the more your vote counts — true believers and long-term hodlers gets more say

Proof of HODL flow

[ephemeral public key] **OP_CHECKSIG**
[timelock] **OP_CHECKSEQUENCEVERIFY OP_DROP**

Demo

Proof Of HODL

Should Bitcoin change its proof-of-work function?

Yes — 2.3 BDL (41.8%)

VOTE

0.05 BTC x 30 days = 1.5 BDL

a day ago

0.02 BTC x 40 days = 0.8 BDL

a day ago

No — 3.2 BDL (58.2%)

VOTE

0.02 BTC x 150 days = 3 BDL

a day ago

0.02 BTC x 10 days = 0.2 BDL

a day ago

vs Bitcoinocracy

Bitcoinocracy lets people vote by signing with their bitcoin private key

- Voting is zero-cost, less reliable signaling
- Shows *current* holdings, not long-term vested interest
- People who are agnostic to the issue have no reason not to sell their vote
- Custodians (exchanges, hosted wallets, etc) can vote with their customers' funds (with proof-of-HODL that would mean running on fractional reserve)

Code on GitHub
https://github.com/shesek/proof-of-hodl

nadav@bitrated.com