Let A

be a sequential work algorithm with constant size intermediary states and solution. (For example let A

be the hashchain proof-of-work algorithm which starts with a seed s

and sequentially computes hashes SHA3^i(s)

for i = 1, 2, ...

. A solution for A

is an integer i

such that SHA3^i(s) < D

for some difficulty D

.)

We propose solution proofs for the sequential work algorithm A

which are constant size and take constant time to verify:

- Crypto-economic proof

: Miners make TrueBit-style claims for solutions to A

. The game validity is asserted and checked in constant space and time.

- Eventually-cryptographic proof

: Miners post collateral promising to deliver, within a certain time period, a cryptographic proof (SNARK/STARK) that a claimed solution to A

is valid. Both the initial crypto-economic game and the final cryptographic proof take constant space, and are checked in constant time. (Notice straight-up SNARKs/STARKs would not be satisfactory because the work to produce them is parallelisable and dominates A

's run time.)