Background

Quantum-secure (asymmetric) signature schemes have 1kB+ signature sizes. The public keys also tend to be large. Wikipedia has a size comparision table for various signature schemes.

Below we combine sequential PoW with a symmetric signature scheme to yield a succinct quantum-secure asymmetric signature scheme. The private and public keys are 32 bytes, and the signature is 64 bytes.

Construction

Let e

be 32 bytes of entropy acting as a private key. Let $H(e)$

be the corresponding public key. Let t

be a transaction with sender $H(e)$

.

The signer first produces a proof p

of sequential work for $[t, e]$

. For example $p = H^n([t, e])$

for some pre-specified large n

. The signature for t

is then $[e, p]$

. Only the first (as recorded by the blockchain) signed transaction revealing e

with a correct p

counts as having a valid signature.

The PoW parameter n

is a security parameter large enough to prevent front-running of the symmetric private key e

on a different transaction t'

.