Stateless SPV proofs (original talk and slides) are an interesting solution from James Prestwich of Summa, to the problem of btcrelay's incentive incompatibility .

To quote from the btcrelay repo:

"the hurdle is when BTC Relay is generating "revenue", then relayers will want a piece for it and will continue relaying, but to get "revenue" BTC Relay needs to be current with the Bitcoin blockchain and needs the relayers first"

How it works

(taken from ZBTC)

Stateless SPV approximates the finality of a transaction based on its accumulated difficulty. Instead of verifying and storing all block headers to date, we compute the cumulative difficulty of a set of headers. As long as the oldest header includes the transaction, and each following header builds upon the last, we can approximate the economic cost to making a fraudulent transaction. The current Bitcoin difficulty, multiplied out by six blocks, can be an approximate cost of Bitcoin's transaction finality. As there is not much material out yet (it was introduced in March 2019), pseudocode below is included to explain better:

def work(header): """Returns CPU work expended in a block header""" assert hash(header) >= header.difficulty return header.difficulty

def cumulative_work(header): if header.prev_block: return work(header) + work(header.prev_block)

return work(header)

def longest_chain(head1, head2): """Determines which head refers to the longest chain of CPU work""" if cumulative_work(head1) > cumulative_work(head2): return head1 else: return head2

This approach is rather bespoke - due to the simplicity of Bitcoin's consensus algorithm, and the network effect of its hashpower, stateless SPV is seemingly secure. If the hashpower were lower, it would be vastly more vulnerable to attacks.

Application to cross-chain proofs

Stateless SPV is a nice approximation on the economic finality of a transaction. It's only useful for simple Nakamoto consensus for now, but if we can produce a succinct ZK proof of Ethash, it could be an interesting approach to proving state on other chains (Cosmos for example) without trusted relayers

.