Firstly, I am aware that using blockhash

for randomness is not suggested, but it is

a viable source of randomness provided that your use of blockhash

does not provide a sufficient financial incentive for miners to try to manipulate blockhash

. For many things, this is entirely sufficient. A simple example is a 50/50 dice roll, with a 2x payout, based on blockhash. As long as the allowed wager is capped at ~(block reward - uncle reward)

, it is not profitable for a miner to try to craft a winning blockhash

. Another example may be using blockhash

to randomly assign items to buckets.

In the sense that there is a real cost to manipulating the value, I call blockhash

an economically staked random number

, for lack of a better term. The ability for contracts to have access to an ESRN exists already in PoW, and there are plenty of reasons for an ESRN to exist in PoS. One being backward compatibility, and another being that it's nice to have access to randomness in a more autonomous way (no extra transactions, no reliance on third parties) – even if there are limitations to how the ESRN can be used

.

I'm not sure how blockhash

is computed in PoS, but if it truly eponymous, then it seems as though validators could trivially created a block with a blockhash

with characteristics of their choosing. In the above examples, they could easily craft a block that wins all rolls, or that distributes all items to one bucket.

I've created an EIP for this here: https://github.com/ethereum/EIPs/pull/1023

What's missing are implementation details.

I'm not sure how the winning validator is chosen in PoS, but I assume there is some process by which the winning validator is chosen without any validator knowing ahead of time who the winner is. Call this randomness data entropyHash

. If validators are required to submit their blocks without knowing the result of entropyHash

, and also if entropyHash

is created using details of the winning block, then it would seem that entropyHash

would be a ESRN

.

Thoughts?

Edit: I'd much prefer this to be a discussion of how randomness can exist in PoS: even if it has limitations (like PoW blockhash

). I'm not interested in discussing why it's "bad practice" to use blockhash

for randomness – it's bad practice only if you ignore the limitations. Let's discuss how we can at least have randomness within some limit.