I have some basic questions about Sentry Node architecture, which is a new concept for me. I'm interested in trying to protect my validator from DDoS and I am looking to get a better understanding about the proper way to set up and configure sentry nodes for mainnet after the secret contract upgrade this month.

1. Do all sentry nodes need to have SGX enabled or is that not required? If SGX is required, are the acceptable values for the isvEnclaveQuoteStatus

field the same as for a validator?

1. How does one determine the optimum number of sentry nodes to include in the validator's persistent_peers

list? Is more sentry nodes always better (other than the increased cost to operate)?

1. Would the validator continue to function properly as long as there is at least one sentry node that is up and running? In other words, would a DDoS attack have to disable all sentry nodes in the persistent_peers

list simultaneously in order to actually disable the validator node?

1. In the event of a DDoS attack on a validator's sentry nodes what is the actual process to respond to the attack? Would one simply shut down the sentry under attack and spin up a new sentry node with a different IP address? Spinning up a new node can take hours - are there any methods to reduce the deployment time?

2. Are there any plans for community sentry nodes perhaps run by the Secret Foundation or Enigma, which would be available to all validators on the network? This would ensure that all validators including those who may not be able to afford running their own sentry node would be able to benefit from the Sentry Node architecture and it would help strengthen the network overall.