majority, thus providing a "decision-discovery" mechanism consistent with the governance mechanism described in the Bitcoin protocol.

Overall, the concept is quite similar to that described in the BIP proposals, except for the fact that the GP is optional in this case and not part and parcel of the main networking protocol. The segregation of the Eleutheros and GP protocols is achieved by adopting a pre-determined value as the "Merkle root of network governance" (a string of 256 zeros).

Not that signals to Eleutheros that there is no network governance input file to be expected (and is to be propagated along with the block contents file, etc.). There is some possibility of a collision i.e. the Merkle root of a network_governance_input file could be a string of 256 zeros, but that's a long shot. We consider that possibility to be extremely remote and not worth giving any consideration. Moreover, if that happens, there would be just one missing vote, and that's the actual concern. The greater concern is to ensure a "missing vote" (whether due to a 256-bit value collision or, more likely, due to a miner deciding not to vote) does not cause vulnerabilities.

With regards to the voting, we anticipate four possibilities:

1. No voice, No vote
If the GP is not used, then the mining software simply writes a string of zeros into the 'Merkle root of network governance' field and that is the end of it. The presence of this string of zeros indicates to other nodes to not expect a "network_governance_input" file. Use cases are "intentionally ungoverned networks" (eg. digital currencies) and other networks where direct network majority rule is unsuitable or undesirable.

2. Emergency stop only
This is when there is a very limited implementation of GP, and the only governance input available to miners is emergency stop. If triggered by a sufficient percentage of the mining capacity, all headers will be invalidated and they will not be appended to the historical blockchain. However, the invalidated blocks won't be immediately discarded but would be retained for further examination. Use case is an emergency of any type (eg Bitcoins 2010 overflow bug issue or Ethereum's 2016 DAO issue[31]), particularly since we cannot assume every network will have 24/7/365 specialized support.

[31] Both were caused by bugs in trust-based applications, not in the trustless network. It is near-certain future blockchain-based applications will have similar issues even if supported by reliable and well-proven trustless blockchain networks, as both are.