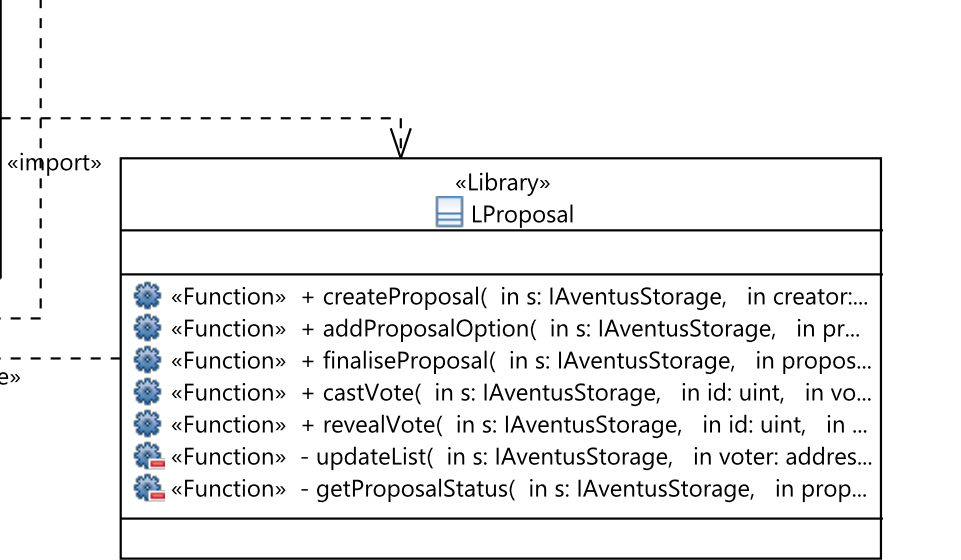
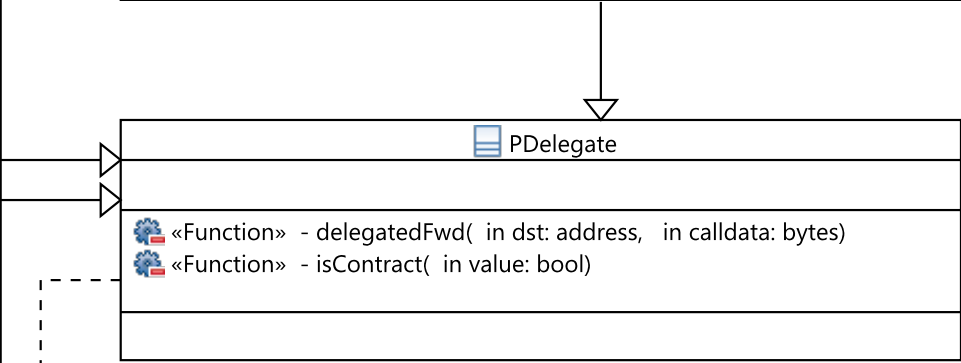
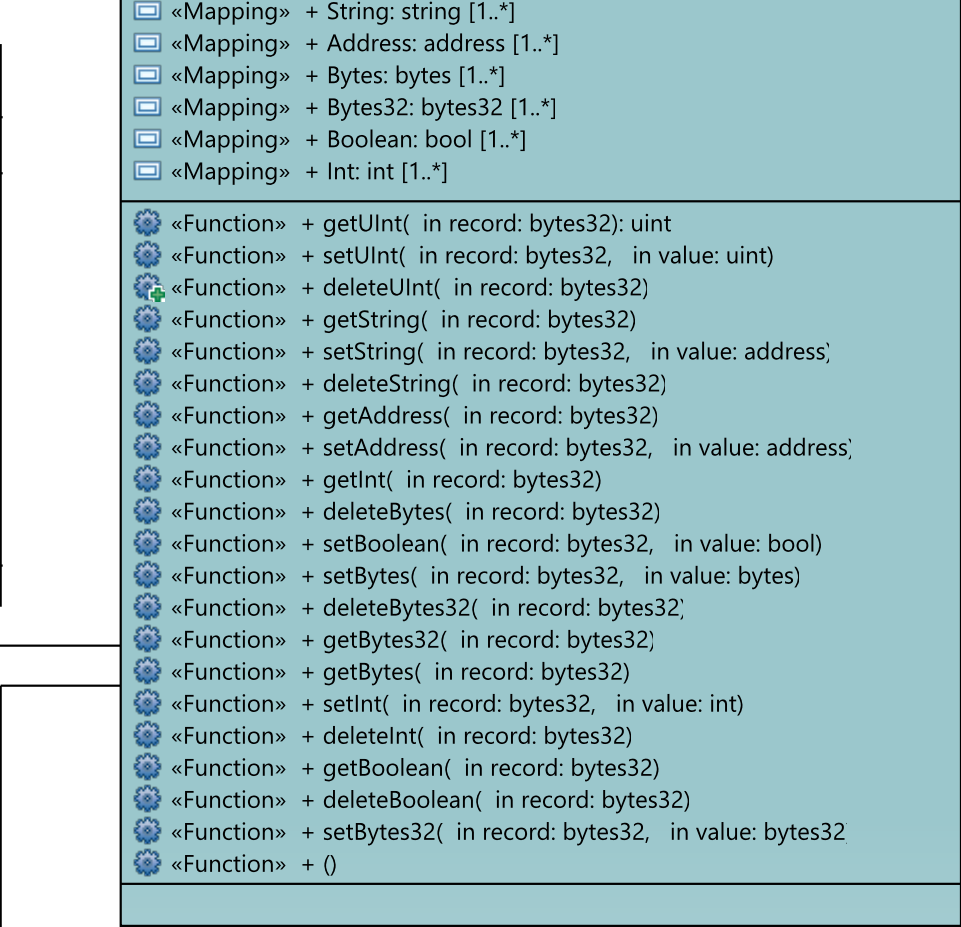
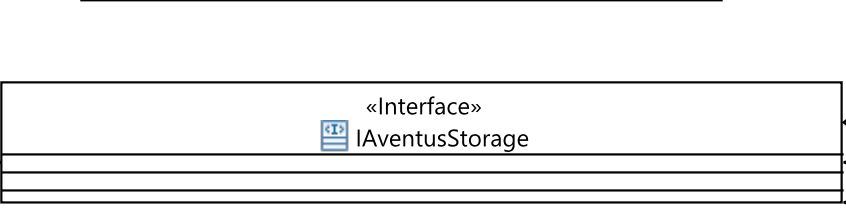
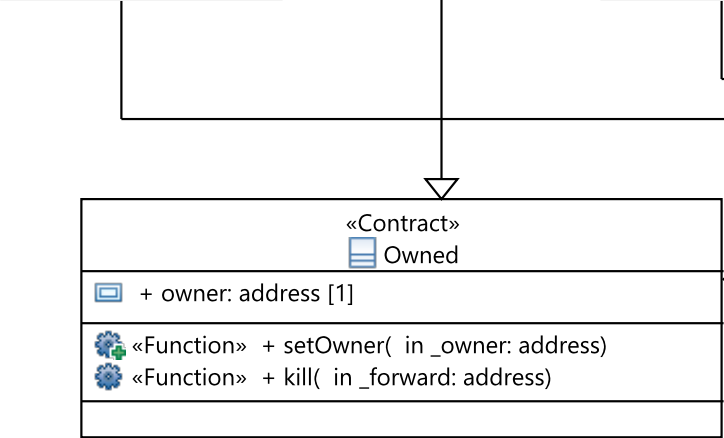
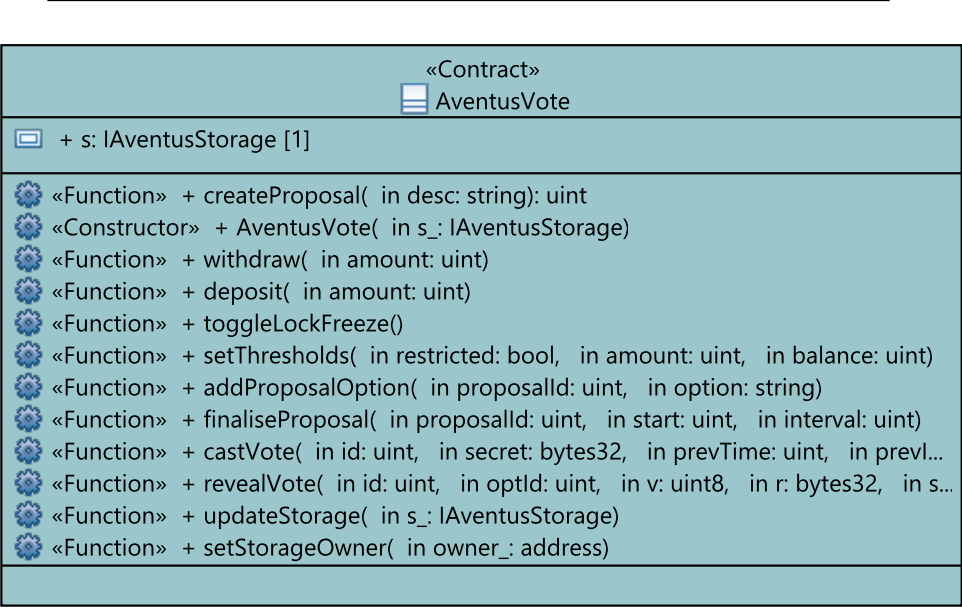


Aventus Voting Protocol
Version: 0.10
Created On: 13 Dec 2017



Proxy extensibility: We need the ability to upgrade library contracts used by the protocol

The problem is when a contract is deployed it is linked to a library at the byte code level. To solve this we link a contract to a proxy contract (the contract appears to reference the library itself in the Solidity code for type safety but we point to the proxy rather than the library itself). The proxy contract has access to a storage contract, which stores a reference to the currently library instance. When a call happens in the top level contract, it delegate calls to the proxy trying to invoke a particular library function, the proxy does not have any function with that signature and so the default function is called, which retrieves the current library instance from the storage contract and delegate calls to that library instance returning the value all the way back to the top level contract. Storage is a special case where we make implement all storage methods and then make it a proxy so that if we extend it in the future it can delegate call to a newer instance with more functionality. This makes every component of our systems upgradeable except for the proxy, but since it just forwards on calls it is unlikely it will ever need to be upgraded.