Basically, everything inside the blockchain is visible, so anyone with access to the blockchain i.e. running a full eth node can dig through the blocks and chain data to get keys out of it, or use [web3.eth.getStorageAt()](https://web3js.readthedocs.io/en/1.0/web3-eth.html#getstorageat)

A solution could be to

* Use a private permissioned blockchain with only permissioned users for protecting confidentiality
* Our solution relies on a combination of rights managements based on Ethereum rights management and using PQ hashing and signatures. Our method protects integrity only i.e. signature matching, since knowing a public key is not enough to violate integrity as no way to know pvt key from public key. Hence integrity is protected even in PQ scenarios