Q i) When is a hash-pointer based implementation of a data structure suitable?

ii) When is a hash-sign-pointer based implementation of a data structure suitable?

A. i) Adding the hash of the pointer's data gives the data structure an added layer of security. In case an adversary wishes to tamper with the data, it would have to recompute the hash-pointer to the node containing the data. This would in turn change the hash of the previous block (the block who's pointer points to the current one), and so on. Thus the adversary would have to recompute the hash value for each node.

case 1: The hash function/key is public. In this case a possible application is to detect disk failure or some sort of errors due to disk degradation.

case 2: The adversary doesnt know the hash function / key of the hash function.
Here there is no way for the adversary to modify the contents since it cannot replace the hash.
Thus an application A_{hash} could be a centralized ledger. For ex- some central authority (like a bank) is the only one with access to the hash function. Any transaction can be recorded by the authority. Since the Data Structure is write-only for adversaries, it is only with negl() probability that one can add an entry by guessing the hash or modifying an entry.

ii) By adding a digital signature as well to the pointer we can track whether an authorized user made the change. For ex- consider A sign to be a ledger of transactions. Now an entry like "A owes B ₹1000" can be added, however it will be trusted only if the entry is signed by A.

This allows the ledger mentioned above to be distributed i.e. each person maintains a copy of the data structure, a transaction when made is signed by the transactee and is broadcasted to the remaining nodes. These nodes can verify the signature and reflect the changes on their local ledger.

of course there is still the issue of conflicting ledgers. This can be solved using for ex- proof of work. In case of conflict choose the copy that has the most work put in. This concept is the fundamental behind cryptocurrency.