How Can Collateral Management Benefit from DLT?

Glossary

Consensus Algorithm
A process, encoded in software, by which nodes in a network agree on validity and order of transactions appended to the ledger

Delivery versus payment (DvP)
A DvP transaction involves the settlement of two linked obligations, namely the delivery of securities and the payment of cash. DvP avoids counterparties being exposed to principal risk, i.e. the risk that the seller of securities could deliver but would not receive payment or that the buyer of securities could make payment but would not receive delivery.

Denial-of-Service (DoS)
A Denial-of-Service attack is a very common method of cyberattack. By sending large amounts of requests to a server in a very short time, the server is not able to keep up with processing the requests and eventually crashes. If the requests are sent from multiple different computers and connections, it is also called a Distributed-Denial-of-Service (DDoS) attack.

Double-spending
Double-spending is an attack where a given set of coins or digital tokens is spent in more than one transaction.

Finality
Finality is a state of a transaction at which point it is guaranteed to be irreversible. In most cases finality refers to deterministic finality which describes a state where there is no possibility of reversing the transaction. In contrast to that, most public blockchains can only reach probabilistic finality, which is defined by the point in time at which the probability of a transaction being reversed is tiny enough that it is reasonable to assume that the reversal is never going to occur.

Hardware Security Module (HSM)
A Hardware Security Module is a device which enables encryption which can only be performed with physical access to it, eliminating the possibility of a remote cyber-attack.

Hash time lock contract (HTLC)
HTLC is a conditional transfer agreement of certain assets where the condition is enforced by the underlying protocol. Time-lock ensures that a transaction is time-bounded: the recipient only has a certain amount of time to accept the payment, otherwise the asset is returned to the sender. Hash-lock prevents counterparties of a transfer to claim the intended assets without fulfilling the conditions stated in the transaction agreement. The combination of hash-lock and time-lock ensures secure asset transfer and can be used for delivery versus payment between different chains/protocols.

Network Operator
The Network Operator is both a technical and a business role. Technically, the network operator is responsible for the infrastructure and makes sure that the nodes can connect to each other. It is also responsible for handling any technical failures which are not limited to one node. On the business side, the Network Operator is responsible for the institutional setup between the participants, it grants and revokes permissions, authorizes updates and handles other necessary auxiliary processes.