How Can Collateral Management Benefit from DLT?

key either on a per transaction basis or with limited time validity. Access control serves a regulatory and organizational role which naturally remains centralized. Participants in a private network who violate network guidelines can be expelled from the network. Through these identifying features, the participants' behavior is traceable and auditable, which is essential for regulators.

Monitoring and Reporting

The network operator should be responsible for monitoring platform health and performance and detecting malicious behavior of nodes. In the latter case, the network operator should also have rights to intervene according to a predefined ruleset. Transaction data should be consistent, and mechanisms must be developed and put in place to prevent fraud and attacks such as double-spending or Denial-of-Service.

For regulatory or supervisory purposes, an Observer Node can be set up which observes the network passively for real-time view of collateral ownership. Additional risk monitoring and reporting applications can be developed to simplify the reporting process and enhance regulatory transparency of the collateral market.

Node Hosting

Participants interact with the distributed ledger through network nodes. The more nodes the network has, the more pronounced the advantages of a distributed network generally are. Participants can run their own nodes, in which case they need to fulfill certain technical and operational requirements to ensure network security, availability and stability. Alternatively, they have the option to access the network through another participant's node or a node hosted by an approved third party.

Security

The security policy has to be extended to the network level in addition to the access control and identity management described above. For example, both inbound and outbound internet traffic have to be filtered and monitored. A multi-level firewall has to be implemented on every node. Peer-to-peer communication between nodes has to be secured and encrypted. A Hardware Security Module (HSM) has become a standard to manage the digital keys. To further reduce risk, nodes can also be distributed physically and geographically.

Outlook: Considerations Regarding Cash in Collateral Management

Within existing collateral management arrangements, cash is an integral element. It is either used as collateral itself or in repo-style transactions as a countervalue to the securities. Cash is available within already established payment systems; the challenge is therefore to integrate cash in a distributed ledger environment.

Cash is usually maintained and transferred within a variety of payment systems of central banks and/or commercial banks involving so-called correspondent banking relationships. Going forward, cash could increasingly be made available for processing within distributed ledger environments. Two options can be considered. Either existing payment systems can be made interoperable with a distributed ledger, or cash can be digitized and directly recorded on a distributed ledger. The latter can either be on-chain issued tokens - so-called native cash tokens – or tokens that represent "classic"