How Can Collateral Management Benefit from DLT?

the Anti-Money Laundering Directive[8]. However, there remain differences in national jurisdictions of member states. Therefore, actors must rely on national legal frameworks where they exist or use contractual arrangements as a legal framework instead. In addition, technology-agnostic regulation for certain existing products may also apply to new offerings on a DLT basis.

5.2   Legal Classification of Tokens

A key question is which rights and obligations are represented by a token. Three broad legal concepts for the nature of a token can be distinguished. Those determine the requirements that must be fulfilled from a legal and regulatory point of view by the various actors of a specific DLT set-up.

The following discrete categories should be considered for tokens related to securities:

(1) Information Token

The least extensive category would be where securities are stored in conventional legacy systems (i.e. a custodian-controlled database, a vault, etc.) and corresponding tokens just carry specific information on these securities. The information stored in the legacy system would take precedence over the information stored on the DLT. And the factual control over the token, or more precisely, its transfer from one participant to another, would not entail a transfer of any rights or obligations with regards to the corresponding security.

(2) Extended Token

In the second category, the same information stored on the DLT would take precedence over the information stored in the legacy system. Control over the security token would provide evidence of rights/obligations regarding the corresponding securities (like for example ownership of the security). However, while control over the token would only *indicate* e.g. ownership, it indirectly *affects* it through an additional legal construct like for example a TTP which ensures that ownership of the security and control over the corresponding token do not diverge. This is because the main legal reference object would still be the security existing outside the DLT Layer.

(3) Native Token

The third and most consequential category would therefore mean the security in total is issued in the form of a token and therefore carries all information as well as all rights/obligations to the security. The legal reference object would be the token and the DLT system itself; any change in token ownership would also automatically trigger legal consequences.

The issuer or creator of the token needs to define the nature of the token in its respective rulebook. The model at hand relates to "(2) Extended Token".

---

[8] The 5th EU Anti-Money Laundering Directive (Directive (EU) 2018/843 of 30 May 2018) introduced a definition of cryptographic values (in the Directive: "virtual currency") and made the safekeeping of cryptographic values subject to certain supervisory requirements.