How Can Collateral Management Benefit from DLT?

Scalability and Performance

Scalability and performance are crucial aspects for business and technology decisions, given that transaction systems can affect critical business processes. Key elements regarding the technical design are data structure, degree of system integration, privacy level and consensus algorithms. These have a direct impact on the scalability and performance of a DLT system. The number of nodes can affect the speed and complexity of consensus building. Therefore, the current number of collateral users and the potential growth in network participants and transactions need to be carefully evaluated while designing and developing the analyzed system. Previous studies have already concluded that current major DLT frameworks such as the Digital Asset Platform, Hyperledger Fabric and R3 Corda are capable of processing current financial transactions and respective volumes[6].

Privacy

Privacy is defined as the right of each individual or legal entity to control the degree to which they are willing to share their personal or business information. In the highly competitive financial market, nearly all information is sensitive. Therefore, any privacy policy has to follow a strict "need-to-know" principle which ensures that all information is only distributed to the relevant parties; at the same time, individuals or organizations are prevented from accessing private data. Sensitive data must be encrypted using certified encryption methods. An optimal solution would also take "forward secrecy" into account, protecting against the possibility of an encryption method being compromised in the future. One way to achieve that is by distributing even encrypted information only on a "need-to-know" basis.

Governance

To properly operate in a regulated environment, the analyzed system needs to have a governance structure. Network participants have to agree on a common platform rulebook and terms of use. Major incidents in the public blockchain sector have made it clear that the "code is law" doctrine is questionable in practice. A governing body is needed to design the system architecture and to define and deploy code, including smart contracts. In addition, there needs to be an authority (e.g. network operator) which manages the admission and permission of participants according to the rulebook (e.g. access rights, read/write abilities, exclusion of participants).

Access Control and Identity Management

In regulated financial market activities, actors need to adhere to strict KYC or AML laws and other regulatory guidelines. For the given scenario, this implies the application of a private permissioned network, where every participant is identified and needs permission to use the service. In general, as part of the onboarding process, a specific network operator registers the public keys of the permitted participants in a whitelist. For privacy reasons the legal entities behind the public addresses in the whitelist might not be known to other participants. To prove identity to other participants for transacting, the system could include a certificate agency and use certificates instead of a static public

[6] See BLOCKBASTER Final Report (https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf)) and DTCC press release (http://www.dtcc.com/news/2018/october/16/dtcc-unveils-groundbreaking-study-on-dlt), Oct 2018