Deloitte.

Regulatory News Alert

The CSSF comes out with its white paper on Distributed Ledger Technology (DLT) & Blockchain use in financial services

27 January 2022

Context

On 24 January 2022, the Commission de Surveillance du Secteur Financier (CSSF) published a non-binding document in the form of a "white paper" aimed at guiding interested professionals in the conduct of their due diligence process related to the Distributed Ledger Technology (DLT) and its use in the provision of services in the Luxembourg financial sector.

DLT: opportunities and a large diversity of applications in financial sector

The potential opportunities offered by the DLT attract an increasing interest from the financial sector (in areas such as initial coin offering, KYC and counterparty or customer identification, collateralization, fund distribution, payment systems, etc.). The financial sector is thus seeing the **emergence of more and more DLT applications and use-cases** to streamline and digitize business processes by limiting or eliminating the need for reconciliations or intermediaries with the help of the DLT.

The CSSF`s white paper aims to ensure that both risks and advantages of the DLT are adequately and appropriately taken into consideration by professionals that considering deploying such solutions in light of the existing Luxembourg laws and future legislative regime at European level.

Key components of DLT

As a starter, CSSF defines the DLT as a technology that allows a network of independent and often geographically dispersed computers to update, share and keep a definitive **record of data** (e.g., information, transactions) in a common **decentralised database** in a peer-to-peer way, **without the need for a central authority**.

There are two key elements that differentiate DLT from traditional databases and qualify a technology as DLT:

1. **Consensus mechanism**[1] used to determine whether a new transaction or record on the DLT is legitimate or not and can therefore be added to the distributed ledger or not; and

2. Use of **cryptography means** to guarantee the immutability (once a transaction is validated and added to the ledger, it can no longer be altered), non-repudiation (authenticity of the accepted transaction cannot be denied) and authorisation (each transaction is acknowledged during the nodes' validation process).

Those key components of the DLT enable transactions and data added to it to be recorded in an immutable way, shared and synchronised instantly across its distributed public or private networks

The risk assessment of the provision of financial services by a regulated entity through a DLT needs to be adapted to different types of DLT architectures since each configuration entails a different set of capabilities and risks.

Roles and responsibilities in the DLT ecosystem

The CSSF has identified the following main roles in the implementation of a DLT-based solution:

- **DLT developer** which *develops the application code* for running the DLT. The DLT developer can be compared to the developer of an operating software. As such, he has to provide updates and fix the vulnerabilities or bugs when they are detected.

- **Infrastructure service provider (ISP)** *delivers the infrastructure on which the DLT runs*. In the case of a public DLT, service providers are free to join and leave the network so there is no contractual relationship possible. A peculiar example of service providers are *miners* which are participating to the network validation based on the incentive of earning block rewards.

- **Solution provider (or software designer)** is the *designer of the "business" solution* which is based on the DLT. He develops *applications for (end-)users* to access the distributed ledger and use the business solution.

- **Users** of the software developed by the solution provider. For example, in the case of a fund distribution platform developed on a distributed ledger, the users would be *regulated entities such as management companies, fund accountants or transfer agents* which contribute to the lifecycle of a fund. The users *provide a service to the end-users*.

- **End-users**, in the previous fund distribution platform example would be *the investors of a fund* managed on the DLT-based fund distribution platform.

When assessing the risks in the provision of financial services through a DLT, it is therefore essential first to identify the participants as well as their role(s) and responsibilities including potential conflicts of interest that may arise when a participant cumulates multiple roles.

Going into the DLT

First, it is a matter of a *strategic decision* to use a DLT to support the provision of financial services, that should be made by weighting the risks against the benefits. The risk analysis should at least cover strategic risks, legal and regulatory risks, security risks, performance risks and confidentiality risks linked to the use of a DLT.

For the purpose of assessing the risks pertaining to DLT and deployment of such technology in the provision of financial services, according to CSSF, the regulated entity should especially focus on:

Governance aspects:

- The chosen *DLT model* will need to fit with the business needs and the regulatory requirements applicable to that entity.

- An entity should consider if the planned DLT-based activities, services or products, *require a license or registration from the CSSF* (for instance, entities

established in Luxembourg or providing services in Luxembourg may not provide virtual asset services without being registered with the CSSF).

- It is recommended to define a person *in charge of any claims related to the malfunctions of the DLT* at the solution provider, ISP and at the developer levels. Also, the dispute resolution mechanisms and the choice of the applicable jurisdiction in case of dispute should be formalized.

- An entity must consider the risk of having to *enforce court decisions* and *block access to assets* stored in a DLT.

- The *legal and regulatory framework* for the use of DLT can vary between jurisdictions and should be analysed (for instance, if smart contracts are used, their legal effect and interpretation should be clear, recognised and formalized).

DLT-specific technical risks:

- The solution provider should verify whether *consensus algorithm has been formally tested* for correctness of operation and *how shortcomings are handled* by this consensus mechanism (for instance in the case of node failures, faulty or malicious nodes) as well as the DLT capacity (volume of transactions).

- Given the specificities of DLT and tokenized solutions compared to more common framework, it is essential to have a proper governance and topology for *node distribution* and *node management*.

- The main questions around *smart contracts* are related to the validation and auditing of the code before its deployment. How is a smart contract validated? What are the frameworks and standards used to ensure the integrity and security of smart contracts?

- Robust *cryptographic keys*[2] management procedures should be put in place (e.g. for the purpose of secure storage of the keys or in case keys get stolen or lost).

- The solution provider should demonstrate measures and controls in place to protect the information about the ownership of the assets, i.e. the relationship between public key and real identity and avoid *privacy and confidentiality risks* to materialize[3]. *AML/CFT regulation* should be fully respected at all times when using the DLT.

Whatever the different actors who are part of the DLT solution are, the regulated entity should still understand these elements and should ensure their appropriate coverage, either directly or indirectly with its subcontractors / partners (solution provider, infrastructure service provider, DLT designer, etc.).

Going forward…

The DLT and blockchain have been recently considered as potentially revolutionary as many practical applications have been identified or developed.

Considerable developments and legislative efforts are emerging **on a European level**. On 24 September 2020, the European Commission published a proposal on a pilot regime for market infrastructures based on DLT. This is comprised in a Digital Finance Package, together with Markets in Crypto-assets regulation (MiCA) and Digital Operational Resilience Act (DORA) that should in all likelihood be up for release this year, thus paving the way for a pan-European market for digital assets in parallel to current legislative frameworks like MIFID or other product regulations.

Deloitte.

From a **Luxembourg perspective**, we should note that there are already laws[4] in place that recognizes DLT and its use in financial services, as well as the tokenization of assets. Hence, there is already a true opportunity to test under a local umbrella new models for trading and custody of digital/tokenized assets.

Finally, the CSSF clearly expressed intention to follow this direction and promote a constructive and open dialogue with Luxembourg financial sector, relying on the local legislative framework to issue new or tokenize assets. With regulations and business converging ahead, we are approaching the cliff edge when **digital models** will become unavoidable and ultimately result in a **significant impact on financial sector**.

Deloitte can help you navigate this new environment, from understanding and defining your digital strategy to enabling the tokenization of assets for financial or other purposes.

[1]In order to validate transactions over a network of untrusted participants, "proof-based" consensus methods are generally used (e.g., Proof-of-Work or a newer generation method, Proof-of-Stake)

[2]In case of loss of the private key, the assets will remain on the blockchain but will be unreachable and unrecoverable by the owner or anyone else, which is a very high-risk unknown in the conventional financial sector.

[3]Regulated entity should define what data to store inside and outside the DLT, assess legal implications including those related to GDPR and take the adequate measures to protect customer data including elements that would make possible to link a customer identity to a public address

[4]The Law of 1 March 2019 and the Law of 22 January 2021, often referred to as the 'Blockchain laws' 1 and 2.

Your contacts

Subject matter specialists

Pascal Martino
Partner – Banking Leader
Tel: +352 621246523
pamartino@deloitte.lu

Thibault Chollet
Partner – Advisory & Consulting, IM & PERE
Tel: +352 621173293
tchollet@deloitte.lu

Laurent Collet
Partner - Banking & Capital Markets
Tel: +352 661451411
lacollet@deloitte.lu

Regulatory Watch Kaleidoscope service

Jean-Philippe Peters
Partner – Risk Advisory
Tel: +352 45145 2276
jppeters@deloitte.lu

Benoit Sauvage
Director – Risk Advisory
Tel: +352 45145 4220
bsauvage@deloitte.lu

Marijana Vuksic
Senior Manager – Risk Advisory
Tel: +352 45145 2311
mvuksic@deloitte.lu

Deloitte Luxembourg
20 Boulevard de Kockelscheuer
L-1821 Luxembourg
Grand Duchy of Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Designed and produced by MarCom at Deloitte Luxembourg