ADAN

L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

Review of Directive on Settlement finality in payment and securities settlement systems

SFD and technological innovation

Answer to the European Commission

May 7, 2021

Adan

Review of Directive on Settlement finality in payment and securities settlement systems

SFD and technological innovation

Adan is thankful to the European Commission for allowing the expression of industry players in this consultation. The Association's objectives are to help create the more favourable environment in the EU for the development of a crypto-asset industry competitive with other regions of the world.

Crypto-assets are improving the existing economic infrastructure worldwide, creating new businesses, helping financial inclusion and providing novel exchange opportunities for both public and private actors. Markets in crypto-assets reflect the growing awareness around such opportunities and the significant traction gained over the last years: the size of tokenized assets markets is estimated to reach 1.4T€ by 2024[1].

The European Commission decided to make financial innovation one of its key priority regarding the importance of making Europe fit for the digital age[2]. As part of the European Union's "Digital Finance" strategy released on 24 September 2020, the European Commission is proposing the creation of a pilot regime for financial instruments issued and traded on blockchain networks ("DLT transferable securities" or security tokens): this transitional regulatory mechanism would (i) allow, along a predetermined period and under conditions, infrastructures to benefit from targeted exemptions of certain requirements imposed by European regulations that are identified as incompatible with technological features of security token activities or not proportionate regarding some obliged entities and (ii) help adjust and build the definitive framework for security token markets based on such experimentation.

This is a significant step in the way of achieving the EU's goal of promoting financial innovation and stopping lagging on the development of the crypto-assets industry behind Asian countries and the USA[3]. Indeed, to be attractive and competitive, the EU must implement harmonized rules for these new markets, but also make the regulatory frameworks and supervisory practices more agile. For years many European actors - both crypto newcomers[4] and significant financial institutions like Société Générale - are on the sideline, waiting for regulatory clarity to contribute to the growth of security token markets. The launch of the pilot regime would release the energy and the creativity of the next European unicorns.

---

[1] Source: Plutoneo Consulting

[2] Ursula Von der Leyen Proposed Program *A Union that strives for more* - political guidelines for the next European Commission, 9 October 2019

[3] The 10 unicorns in the sector are incorporated there, and large-scale operations are happening in those jurisdictions. As an example, the HSBC-Singapore Exchange-Temasek (owned by the Singaporian State) partnership recently successfully executed a $294 million bond issuance on blockchain.

[4] In a recent survey conducted notably by the French professional association ADAN, 42 companies reported that they were implementing security token projects, among them: Equisafe, Société Générale – Forge, GT Equity, Kaiko, OFI, Tokeny and WeFundia. More details on their activities can be found in the synthesis report: https://pages.adan.eu/rapport_security_tokens_cadre_europe_en

To this end, the Settlement Finality Directive (SFD) review must be part of this dynamic and support coming efforts to let the EU embrace innovation by appropriate and proportionate adjustments.

Adan is available for any question and further discussions related to this paper.

Adan answers

Question 3.1 Do you consider the SFD to be technologically neutral?
- Yes, everything is sufficiently clear no matter the technology used.
- No, I do not know how to apply certain concepts or definitions of the SFD for specific technologies which creates legal uncertainty (please explain under question 3.5.).
- Don't know / no opinion / not relevant

SFD cannot be technologically neutral because finality makes different senses for "traditional" transactions and those settled on blockchain networks ("on-chain transactions").

Legally speaking, the finality of transactions refers to the "delivery versus payment", defined in article 2.27 of CSDR as "a securities settlement mechanism which links a transfer of securities with a transfer of cash in a way that the delivery of securities occurs if and only if the corresponding transfer of cash occurs and vice versa". This concept is also covered by PFMIs 8 and 12.

Technically speaking, in the blockchain universe, the finality of transactions is always technically probabilistic, regardless of the system used for their recording.

Transactions on crypto-assets (including security tokens) are validated by consensus, a mechanism by which a distributed network of nodes agrees on the only valid version of a distributed ledger. There are many consensus protocols, among the best known: proof of work (Proof of Work - PoW), proof of stake (Proof of Stake - PoS) and proof of authority (Proof of Authority - PoA) .

PoW does not currently offer a strict finality of transactions. Theoretically, there should be only one version of the register to be accepted by all participants. However, divergences may emerge within the community and a (or a subset of) node(s) may decide to continue to valid transactions on a version of the ledger different from the one used by the majority of network nodes.

When two versions of the same register co-exist, the longest chain should be considered the only source of truth. Two main pitfalls then arise. On the one hand, this version may take some time to propagate in the network and uninformed participants can refer, in good faith, to the shortest chain. However, transactions that have been validated by the "losing" chain will ultimately be considered null and invalid, unless these transactions have been validated by the "winning" chain.

The finality of transactions on a blockchain operating on the basis of the PoW consensus protocol can therefore be difficult to guarantee. In the face of such uncertainty, some good practices have spread across the community. Vitalik Buterin, founder of the Ethereum blockchain, has thus determined - on

the basis of probabilistic calculations - that a transaction can be considered final after six confirmations[5].

In addition to the proof of work, other consensus protocols make it easier to reach the finality of the transactions. In the case of proof of stake, competition between several chains is impossible because two thirds of validators must validate a transaction for it to be considered final. Consensus mechanisms operating on proof of authority (such as RAFT or IBFT) have a limited number of potential validation nodes, allowing them to more easily check to what extent the majority of validation nodes have agreed on a given block. Regarding the latter, their adoption is limited: on the one hand, they tend to become unstable when several tens of validation nodes are involved; on the other hand, a limited number of validating nodes increases the probability that they take control of the network.

The compatibility between the technological finality of on-chain transactions and the legal finality raises several questions.

First, as described above, the finality of transactions can be affected by the validation protocol. In the most frequent case of PoW, waiting for a certain number of confirmation so that the probability that the transaction can be revoked becomes negligible might seem insufficient, market participants needing certainty at a given point in time rather than on the basis of probabilities. Certain characteristics intrinsic to blockchain technology - the possibility of forks, the variable speed of validation depending on the channels (and especially their inconstancy) - heightens the uncertainty as to when the finality of the transactions can be attested. The other consensus protocols, such as proof of stake and proof of authority, could be better perceived by these actors, provided that their adoption is currently limited.

Second, at this stage, the lack of legal tender money on the blockchain prevents the full decentralized delivery versus payment of security tokens. It can be made possible using stablecoins, but these assets are authorized in the current legal framework. Consequently, the securities leg and the cash leg of a transaction on security tokens must be managed simultaneously, respectively on the blockchain and on the bank accounts kept by credit institutions: each transaction signed on the blockchain where the financial tokens circulate must be associated instantly with the payment. Under these conditions, the finality of the transactions can be longer to establish.

Question 3.2 Do you agree that the concepts of the SFD do not work in a permissionless DLT environment?
- Yes, important concepts of the SFD do not work in a permissionless DLT environment, especially as legal responsibilities might be unclear. It is indeed problematic that there is no centralised operator, unidentified participants can enroll without restriction and functions can be attributed simultaneously to several participants.
- No, I do not see any problem to apply the concepts of the SFD in a permissionless DLT environment. (Please provide detailed information of how you think settlement finality under the SFD can be achieved despite the lack of a centralised operator, the fact that

---

[5] https://blog.ethereum.org/2016/05/09/on-settlement-finality/

unidentified participants can enroll without restrictions and that functions can be attributed simultaneously to several participants.)

- Don't know / no opinion / not relevant

Question 3.2.1 Please provide detailed information on your answer to question 3.2:

As stated in our answer to question 3.1, (permissionless) blockchain technologies enable achieving transaction finality. Technically speaking, the "lack of a centralised operator," "unidentified participants can enroll without restrictions" and "functions can be attributed simultaneously to several participants" do not threaten achieving settlement finality.

Therefore the problem does not lie with the DLT environment but rather with necessary adjustments to SFD to allow the use of such technologies. This could require designing conditions to be met by such technologies. Please refer to more details on:

- Adan's proposed methodology in our answers to question 3.4 and 3.5.
- Such conditions in our answer to question 3.6.

Question 3.3 Do you agree that the scope of the current review of the SFD should be limited to considering the tech neutrality of the SFD in the context of permissioned DLTs where the system operator could design the system and its rules so as to be SFD compliant?

- Yes
- No
- Don't know / no opinion / not relevant

Question 3.3.1 Please explain your answer to question 3.3:

Based on explanations given in our answer to questions 3.1 and 3.2, the scope of the current review of the SFD should not be limited to considering the tech neutrality of the SFD in the context of permissioned DLTs. Permissionless DLTs should also be considered.

Generally speaking, the commonly-used binary distinction between so-called "private" and "public" blockchain networks fails to capture the possible nuance between these extremes. Instead, one should look at blockchain networks as being more or less open, a function of how said blockchains configuration.

When interacting with a blockchain network, there are three broad roles one can assume:

- transaction validator, such as mining or approving blocks by participating in consensus;
- application developer, such as developing and deploying smart contracts, and;
- application user, such as sending and receiving transactions, and interacting with applications.

These roles may overlap as one may assume different functions (e.g., block validation activities require sending and receiving transactions).

ADAN
L'ASSOCIATION POUR LE DÉVELOPPEMENT DES ACTIFS NUMÉRIQUES

While typically, blockchains networks either allow full open access to all three of these roles (so-called "public" blockchain networks) or restrict access to authorised entities (so-called "private" blockchain networks), there exist practical and theoretical examples where the public/private classification is not so clear. Much like the Internet, built on open protocols and standards (e.g., TCP/IP, HTTP, SMTP), and open networks operated by private enterprise, open blockchain networks can support production applications with universal access.

Question 3.4 Do you think that first experience with the pilot regime for market infrastructures based on DLT (COM/2020/594 final) should be gained before considering possible issues in the SFD?

- Yes, this will show problems resulting from the use of DLT that have to be considered in the SFD.
- No, there are already issues which have to be addressed for the use in a DLT environment as they currently create legal uncertainty.
- Don't know / no opinion / not relevant

Question 3.4.1 Please elaborate on your answer to question 3.4, if necessary:

The European Commission has engaged several positive steps to better consider the crypto-asset innovation, from the pilot regime proposal to the dedicated focus within the CSDR, SFD and FCD consultations.

Nevertheless if some issues have already been identified, the current pilot regime proposal does not allow to explore and implement necessary exemptions to SFD to authorise the use of blockchain technologies. Moreover, innovation is moving constantly so not all stumbling blocks in SFD can be identified as of today. Finally, as other legal obstacles hamper the development of security token markets (especially regarding secondary markets - MiFID2 and CSDR), it is likely that additional deadlocks in SFD will be experimented when innovation will no longer be limited by such grey areas.

That is why the SFD review should not only, in a short term vision, resolve legal obstacles due to incompatibilities with the functioning (they cannot all be anticipated) but also consider, in a long term vision, how blockchain technologies and crypto-assets meet the objectives set by financial regulations in order to adapt and rationalise SFD rules permanently and efficiently. If blockchain technologies and tokenization find another way to achieve such objectives (e.g without centralised operators), regulations should adapt not to hinder their potential for innovation.

To this end, the pilot regime is the most appropriate regulatory tool. Accordingly the pilot regime should also include SFD considerations and the SFD review should coordinate with the pilot regime roadmap. This pilot regime is a positive starting point but efforts should be maintained to refine this proposal and make it more flexible. At this stage, possible experimentations and exemptions are very restricted. It is crucial to open this scope to be able to expand it following the pace of innovation. For more details, Adan conducted a deep analysis of the pilot regime and suggested some improvements in the context of the European Commission's feedback period closed in January 2021.

Question 3.6 Are there any other amendments to the SFD that should be considered to deal with opportunities and/or risks that are specific to a permissioned DLT based SFD system?
- Yes
- No
- Don't know / no opinion / not relevant

Question 3.6.1 Please explain the risks and how they might be mitigated in the SFD:

As explained in our answer to question 3.5, not all required amendments to the SFD can be anticipated today in order to allow transaction finality in a DLT environment. Questions asked in the consultation document focus on already identified and very particular issues raised in SFD because of the specific technical features and functioning of crypto-assets. This is one line of attack but this can be the main one.

A purpose-based regulatory approach would be better adapted in order to determine necessary legal adjustments for security tokens based on guarantees brought by the technological features of blockchain networks and optimise rules thanks to blockchain benefits. To this end, permissionless networks should not be set aside from such amendments.

Obviously optimising the current regulatory framework for market infrastructures must be associated with all new required and useful guarantees allowed by innovation. To this end, regulators could capitalise on smart contracts opportunity enabling to automate conditional behaviours by encoded adequate counterparts to legal adjustments (insurance, guarantees, etc.). New blockchain tools can also be very relevant to provide for necessary guarantees (blockchain analytics, smart contract auditing, dedicated insurance, etc.).

About Adan

Adan (Association for the Development of Digital Assets) is a non-profit bringing together and representing crypto-assets and blockchain professionals in France and Europe. Adan's members cover a wide range of activities: crypto-asset markets, custody, payments, investment management, blockchain analysis tools, support for crypto/blockchain projects, IT security, etc. Adan's mission is to promote the development of the crypto-assets industry in favour of a new digital economy.