The Formation and Execution of Contractual Securities through Smart Contracts under Luxembourg Law

Théo Antunes

Abstract: Smart contracts, with their self-executing nature and reliance on blockchain technology, provide financial professionals with increased efficiency, transparency, and security in executing contracts, particularly in cases of debtor default in the context of contractual securities. Traditional securities require manual processes such as document signing, obligation verification, and potential court involvement in disputes, whereas smart contract securities execute automatically, ensuring prompt fulfilment of obligations without human intervention. Despite these significant advantages in time management and legal certainty, implementing smart contracts within the context of Luxembourg's security laws meets substantial technical and legal challenges.

Firstly, the inherent rigidity of smart contracts contrasts with the flexible and interpretative nature of legal securities. Securities law often necessitates adaptability to address unforeseen circumstances and equitable considerations, which are difficult to encode into the binary logic of smart contracts. This rigidity can result in automated executions that fail to reflect the nuanced intentions of the parties or changing conditions, potentially leading to unjust outcomes.

Secondly, Luxembourg's current legal infrastructure lacks comprehensive regulatory guidance specific to blockchain and smart contracts in this context. This regulatory gap creates uncertainties regarding the legal recognition, enforceability, and interpretation of smart contracts under contractual securities law. While Luxembourg fosters a fintech-friendly environment, the rapid advancement of blockchain technology outpaces the adaptation of legal frameworks, underscoring the need for targeted legislative and regulatory efforts to align innovative technologies with traditional legal principles.

Thirdly, the challenges faced by Luxembourg are echoed throughout the European Union, where a harmonized approach to blockchain and smart contract regulation is still developing. The European initiatives, such as the Digital Finance Package, the electronic IDentification, Authentication and trust Services regulation, and the Market in crypto-assets regulation, aim to create a cohesive regulatory environment. However, integrating smart contracts into existing legal systems, especially in areas like securities law, requires further detailed regulatory efforts. The purpose of this article is to emphasize a comprehensive regulation of the establishment and execution of securities through smart contracts under Luxembourg law. It also explores the potential opportunities offered by smart contracts, particularly considering the degree of flexibility required for different types of securities under Luxembourg law.

I. The intersection of securities' law and smart contracts under Luxembourg law

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically enforce and execute actions when predefined conditions are met, without the need for human intervention or intermediaries.[1] They run on Distributed ledger technology (DLT) networks aiming at ensuring transparency, security, and immutability of the agreements built on them.[2] Such a definition presents smart contracts with several criteria: They are contracts, they are automated, immutable, and their execution is delegated to algorithms built on DLT. Each of these aspects presents challenges under Luxembourg law, for they intersect between traditional written contract law and new technologies relying on such a technology.[3]

Securities law is deeply linked with contract law, for securities aim at ensuring that the creditor will have compensation in case where the contractual obligation of the debtor is not fulfilled. As such, they are also bound by the principles of contract law, such as contractual freedom, the existence of an agreement, and the enforceability of the contract between the parties.[4] Because they are dependant to contracts, securities cannot exist without them.

However, the particularities of smart contracts lead to rethink the way securities can be formed and executed in the DLT environment, what are the challenges and the limitations that they can be subjected to. On one hand, Luxembourg's legal framework has known a rapid awareness to DLT used by financial professionals in several contexts (A). On the second hand, one needs to assess such framework with the lens of securities law to assess at what extent does the Luxembourg legal framework can encompass them in smart contracts (B).

1 Weiqin Zou and others, 'Smart contract development: challenges and opportunities' (2021) *Research Collection School of Computing and Information Systems* 1–22, 1; LetzBlock, *Smart contract: a Luxembourg perspective, assessing opportunities and key legal challenges* (Smart Contract Working Group 2021) 1–68, 7.

2 LetzBlock, *Smart contract: a Luxembourg perspective, assessing opportunities and key legal challenges* (Smart Contract Working Group 2021) 1–68, 13

3 Elise Melchior, 'Réflexions juridiques autour de la blockchain : analyse sous l'angle du droit des contrats' (2018) 72 *Revue du droit des technologies de l'information* 45–65, 53

4 Luxembourg Civil Code, article 1108.

A. Clarifying the formation and execution of securities in Luxembourg through smart contracts.

Financial securities are crucial for the Luxembourg's financial sector. They aim at securing that the creditor can be compensated in cases where the debtor fails to fulfil the obligations inscribed in a given contract.[5] Several financial securities exist in Luxembourg, and they adapt to different sort of situations, whether mortgage, financial guarantee contract, a pledge, transfer of property targeting financial assets, collateral… Securities are adapted depending on the contract they are inserted in, the business relationship, the parties in order to ensure for both the creditor and the debtor an adequate contractual framework. For instance, mortgage is common for real estate loans, and transfer of assets as collateral are common for loans involving asset managers to credit establishments. Each type of security aims at answering an adapted contractual relationship between a debtor and a creditor.

Because of such flexibility, the formation and execution of securities differ depending on the selected one, they are nonetheless framed by the same principles. These principles aim at making these securities contractually legal (1). Moreover, the recent years have shown a rising flexibility for financial professionals to form and execute securities (2).

1. Principles of formation and execution of securities in Luxembourg.

What are the principles framing the formations and executions of securities? Since both the formation and execution answers to different objectives, their principles differ according to Luxembourg contract law, which securities are bound to. Hence it is necessary to distinguish between these two. Securities are framed by three distinct criteria: the purpose of the security, its effect and the technique used to form it.[6]

Firstly, the formation of securities in Luxembourg is bound to the same principles than the contract it depends on. Securities are governed by the general rules of contract formation. According to article 1108 of the Civil Code, "*four conditions are essential for the validity of an agreement: the*

5 Antoine Cuny de la Verryère, *Sûretés et garanties au Grand-Duché de Luxembourg* (Larcier Luxembourg 2018) 26.

6 Pierre Crocq, *Propriété et garantie* (LGDJ 1995) 248.

consent of the party who undertakes the obligation; their capacity to contract; a certain object which constitutes the subject matter of the commitment; and a lawful cause in the obligation".[7] In the context of forming securities however, further clarifications need to be made. Contractual freedom entails the consent of the parties to have recourse to securities as part of the contractual clauses. Thus, according to contract law, this means that the debtor's consent must be free, meaning that it should not be subject to any coercion, violence or misleading attempt from the creditor.[8] The object, for its part, must be lawful, possible, and determinable.[9] The cause of a security interest generally lies in the payment of the principal debt.[10] Moreover, parties must have contractual capacity, which is divided into the capacity to enjoy rights, on the one hand, and the capacity to exercise rights, on the other. It is negatively defined by article 1124 of the Civil code entailing that some categories of populations, such as underaged, the persons that are forbidden to contract and generally all people whom the law forbid to contract.[11]

Those four principles entail that both the creditor, but especially the debtor, needs to be fully aware of the ramifications that such security entails and the conditions for its execution. If these principles frame the formation of securities, they must also answer to further requirements under Luxembourg's law, depending on their nature. For instance, if most of the securities require proof of the failure of the debtor to uphold its obligations to be executed, some can be executed before bringing such proof such as the "*Garantie à première demande*".[12] It would be then up to the creditor to demonstrate such failure, but such *ex-ante* execution can be harming for debtors that are not fully aware of the implications of this precise security. When assessing the consent under contract law, one could see that it is be limited to the object of the security as well as its execution. The form of the security is often required to be written and clear enough to avoid any misleading from the creditor. But the written form *per se* does not fall under the appreciation of the consent, only its content and the way it is executed.[13]

7 Luxembourg Civil Code, article 1108
8 Luxembourg Civil Code, article 1109,
9 Luxembourg Civil Code, article 1110
10 Luxembourg Civil Code, article 1131
11 Luxembourg Civil Code, article 1124
12 Court of Appeal (Luxembourg), 16 March 1983, *Droit et Banque* No 2, 39, para 25.
13 Philippe Ancel, *Contrats et obligations conventionnelles en droit luxembourgeois* (Larcier 2015) 261–332, 269.

To fully assess the formation of securities in Luxembourg, one must also consider the application and evolutions of the law of 2005 on financial securities, expanding the number of securities available for financial professionals under commercial law.[14] Among them, the pledge on assets can take the form of share pledges, pledges on receivables or pledges on account. They answer to special rules for the formation of the security that the contract must upheld. A dispossession must occur, under which the debtor transfers the possession of the financial assets to the creditor, meaning that the debtor be the owner of those assets.[15] Another one yet, the transfer of ownership is another security enshrined in article 13 of the law of 2005, it entails that on the one hand, it involves an assignment mechanism whereby ownership of assets is transferred to the beneficiary of the security to secure the financial obligations of the grantor.[16] On the other hand, it includes a reassignment mechanism, where the assignee commits to transferring back the assets or equivalent assets at an agreed date, except in the event of total or partial non-performance of the secured financial obligations. Thus, this law entails specific rules on the formation of these securities, detailing precisely how the formation should occur, pending that they also answer to the principles of article 1108 of the Civil code. More recent yet, the law of 10th July 2020 brings a new type of security, the professional payment guarantees, whose modalities are let free to the parties, guaranteeing more freedom for its formation and execution, pending that they are also framed by the principles set forth by article 1108 of the Civil code.[17]

Secondly, the execution of securities is dependent on the failure of the debtor to uphold its contractual obligations.[18] As mentioned above however, such failure can be demonstrated with a certain extent of flexibility, especially considering what and when the security can be executed. The law of 2005 also attaches special rules for the securities it enshrines. For instance, a triggering event that leads to the enforcement of the security, as stipulated by the agreement, must have occurred, notably concerning

14 Loi du 5 août 2005 sur les contrats de garantie financière, articles 2, 3, 13.

15 Loi du 5 août 2005 sur les contrats de garantie financière, article 5 (1); Antoine Cuny de la Verryère, *Sûretés et garanties au Grand-Duché de Luxembourg* (Vademecum Larcier Luxembourg 2018) 61.

16 Loi du 5 août 2005 sur les contrats de garantie financière, article 13

17 Armel Waisse and Laurent Henneresse, 'Luxembourg: law of 10 July 2020 on professional payment guarantees' (2020) *Eurofenix: Country Reports 2020/21,* 41

18 Antoine Cuny de la Verryère, *Sûretés et garanties au Grand-Duché de Luxembourg* (Vademecum, Larcier Luxembourg 2018) 35.

the pledge security.[19] This triggering event must be precisely defined and can consist of multiple causes: a change of control, deterioration of the debtor's financial ratios, default on payments related to the underlying credit agreement or a related contract, meaning the failure to pay commissions to third parties involved in the financing operations. The triggering event defined by the parties constitutes an autonomous realization event, breaking with the requirement for the secured debt to be due. Luxembourg law, therefore, allows for the enforcement of a pledge even in the absence of the secured debt's maturity, they can be two different events if they are explicitly inscribed as such by the security triggering event.

2. Smart contract and securities: What are we talking about?

The use of DLT as a mean to form and execute securities imply that they are registered and signed digitally by the parties.[20] The main opportunity of such endeavour lies in its execution, where the smart contract, on one hand assess autonomously whether the conditions for the execution of the securities are met and on the other hand, proceeds to the execution of the security to the profit of the creditor.[21] For instance, in the case of a mortgage, the transfer of the deed of the ownership of the house could be transferred to the credit establishment in cases of failure of the debtor to uphold its obligations. This mechanism requires several requirements larger than the establishment of the smart contract.

Firstly, it requires a certain extent of tokenization to allow a transfer of the collateral pursuant to the security agreement.[22] Indeed, to operate adequately and according to its nature, the smart contract needs to have collateral available for its automated transfer in case of the debtor failure to uphold its contractual obligations. Operating on a DLT requires the funds to be operating on it as well. Hence, whatever the collateral is, it needs to be on the same layer as the contract, meaning the same DLT. As such, the collateral can take the form of crypto-assets, tokenized financial assets, tokenized deeds of property such as ownership of real estate or other types

19 Loi du 5 août 2005 sur les contrats de garantie financière, article 11(5).

20 Deutsche Börse AG, *How can collateral management benefit from DLT* (Deutsche Bundesbank Project 'Blockbaster' 2020) 1–21, 4.

21 Howard Altarescu and others, *Finance, securitization and smart contracts: business white paper* (MOBI 2021) 1–27, 14.

22 ISDA, *Private international law aspects of smart derivatives contracts utilizing distributed ledger technology: French law* (2020) 1–21, 17.

of financial assets that underwent the process of tokenization. Thus, the setting up of a smart contract for the execution of securities previously requires a process of a certain extent of tokenization from both the debtor and the creditor.

Secondly, to form the smart contract, the parties must agree on the type of security they would like the smart contract to execute, the stakes, the triggering event and all the conditions depending on the nature of the security at stake. It must be done in compliance with the formal legal requirements depending on such choice. However, this must be done in full compliance with the applicable laws and by reference to article 1108 of the Civil code. Such a position implies that a smart contract is not fundamentally different from the process of formation of a traditional contract, it just occurs on a different format.[23] However, the main difference lies in the immutability of the software, meaning that once it is written up on the DLT, will not be possible for the parties to change the terms of the security nor its execution.

Thirdly, the main point differentiating smart contracts from traditional execution of securities, the execution is totally outsourced to the smart contract programming.[24] This means that the triggering event, the determination of the failure of the debtor as well as the transfer of funds, assets or the deeds are done without any human intervention. The program should be able to assess whether the debtor is upholding all his obligations and whether the requirements for the triggering event has been met. The execution of the smart contract makes the recovery of the collateral faster for the creditor, but it also requires a certain amount of trust in the programming, needing it to be properly programmed to be executed as the parties intended. Decentralized autonomous organizations already make use of smart contracts to ensure the formation and execution of securities by taking crypto-assets as collateral before accepting a further transaction.[25] This type of organization is totally decentralized, meaning it operates with

23 Elise Melchior, 'Réflexions juridiques autour de la blockchain : analyse sous l'angle du droit des contrats' (2018) 72 *Revue du droit des technologies de l'information*, 45–65, 54–55.

24 Stuart D Levi and Alex B Lipton, *An introduction to smart contracts and their potential and inherent limitations* (Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates 2018) 1–11, 3.

25 Juliette Sénéchal, 'Blockchains « publiques », smart contracts, organisations autonomes décentralisées et gouvernance' in *Les blockchains et les smart contracts à l'épreuve du droit* (Larcier 2020) 51–97, 68.

a central governing authority. MakerDAO for instance manages the Maker protocol enabling users to generate DAI stablecoins.[26] Users who want to generate DAI can do so by locking up cryptocurrencies in a smart contract as collateral. In exchange, they receive DAI tokens, which they can use freely. If the value of the collateral falls below a certain threshold, the system automatically liquidates the collateral to ensure that DAI remains fully backed.

One could see that this third step fundamentally differs from the traditional approach of securities, as the program should, in principle, be allowed to assess whether the debtor is upholding his obligations by itself. This requires a certain autonomy from the program to both recognize the triggering event as well as executing the full security as agreed upon by the parties.

B. Addressing the regulatory landscape for smart contracts and securities

DLT has gained a lot of awareness in the past years, both from regulators perspective and financial professionals alike. They show promises for financial professionals, whether by automating processes, tokenizing financial assets, better communications for whistleblowing channels or as a mean for expanding their activities with the rise of crypto-assets, cryptocurrencies and at some extent, non-fungible tokens. This technology was addressed at the European level as part of the digital finance strategy, aiming at providing renewed digital infrastructure for financial professionals, enhance financial inclusions for consumers and bolstering the financial flows within and out of the EU.[27] As such, the Luxembourg approach of DLT and blockchain regulations is delved within a European dynamic to regulate such technology for financial purposes (1). Such dynamic was enshrined in Luxembourg's law, notably since 2019 with four "*Blockchain law*" for DLT application by financial professionals (2).

1. A European dynamic

Lately, the EU has undertaken a regulatory approach aiming for the regulation of digital finance. Whereas no binding instruments is directly reg-

26 MakerDAO Maker Team, *The Dai stablecoin system* (White Paper 2017) 1–21, 3–5.

27 European Commission, 'Digital finance strategy for the EU' COM(2020) 591 final, 24 September 2020.

ulating the use of smart contracts, European norms tend to apply in a general and special approaches.

Firstly, several regulatory texts aim at framing the deployment of DLT for financial professionals. Since smart contracts often contain personal data, for the sake of its normal functioning (such as bank coordinates, name of the parties, addresses...) any smart contract that processes personal data must ensure compliance with General data protection regulation (GDPR) requirements, including obtaining explicit consent from individuals and ensuring data protection by design and by default.[28] Because of their digital nature and their reliance on Blockchain, a cryptographic key is needed to prove ownership or authorization to undertake transactions pursuant to the smart contract, one needs to have a cryptographic key, requiring an electronic signature that must be compliant with the electronic identification and trust services (eIDAS) regulation to ensure those signatures are legally recognized across the EU.[29] To rely on smart contracts to form and execute financial securities also entail a compliance with Digital operational resilience act (DORA)'s standards for operational resilience, ensuring the system is safeguarded against cyber-attacks aiming at changing the content of the smart contracts or redirecting the funds.[30] To the extent that the smart contracts involve consumer transactions, for forming and executing securities related to mortgage for instance, credit establishments need to provide clear information and respect the consumer's right to withdraw under certain conditions in compliance with directive 2011/83/EU on Consumer's right.[31] This bundle of hard-law frames the application of DLT for securities at the European level, nevertheless it requires a challenging cross-analysis of these norms to ensure its compliance with European rules. the Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology aimed at providing common standards for providing market infrastructure relying on DLT, to assess the feasibility of the standards and the practical challenges associated with it.

28 Michèle Finck, *Blockchain and the General Data Protection Regulation: Can Distrubuted ledgers be squared with European Data Protection Law Study* (European Parliamentary Research Service, July 2019) 6.

29 European Law Institute, *ELI principles on blockchain technology, smart contracts and consumer protection* (Report of the European Law Institute 2023) 1–52, 15.

30 Giuseppe Siani, *Regulating new distributed ledger technologies (DLT): market protection and systemic risks,* Speech, (Banca d'Italia Eurosistema 2022) 1–12, 4.

31 Directive 2011/83/EU on consumer rights [2011] OJ L 304/64, article 6.

Furthermore, these binding norms must be read together with approaches undertaken by the European Commission and the Parliament on Fintech and DLT technologies. These documents act as guidance aiming at precising the European expectations in the field of DLT applications. Among them, the European Parliament Resolution on Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation,[32] the Digital Finance Strategy for the EU (2020), the Blockchain and the GDPR, EU Blockchain Observatory and Forum (2018), the FinTech Action Plan: For a More Competitive and Innovative European Financial Sector (2018) and the Shaping Europe's Digital Future (2020)L Together, they aim at providing guidance on the expected standards that DLT should adopt at the European level. Several principles are enumerated, among them: transparency, cyber-security or compliance with AML norms. This European framework aims at establishing a European DLT ecosystem, mostly in cases where it is used as a new market infrastructure, meaning a support for transaction flows constating in tokenized or crypto-assets. This European dynamic is completed with a Luxembourg's one, demonstrating the will for the Luxembourg legislator to directly frame the use of DLT in the financial sector.

2. A Luxembourgish dynamic

Luxembourg has been proactive in its regulation of DLT used in the context of financial acuities. Commonly referred to as "*Blockchain laws*", Luxembourg has been at the foremost of DLT regulation in the financial sector.

The Blockchain Law I of the 1st of March 2019 was one of the first in the EU to equate blockchain in the context of traditional transactions, allowing the use DLT for account and financial assets registration.[33] The Blockchain Law II of 22nd January 2021 further supported dematerialized assets by enabling secure electronic registration on DLT and broadening access to financial institutions.[34] The Blockchain Law III of 14th March 2023 enhanced this framework by updating securities laws, aligning with EU regulations,

32 European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation [2020] OJ C 11/3.

33 Loi du 1er mars 2019 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres.

34 Loi du 22 janvier 2021 portant modification : de la loi modifiée du 5 avril 1993 relative au secteur financier et de la loi du 6 avril 2013 relative aux titres dématérialisés.

and redefining financial instruments to include DLT. It notably updated the 2005 Law on Financial securities arrangement allowing use of electronic DLT for collateral over financial instruments held in securities accounts. This law opens the door for securities registered on DLT, but do not address the formation and execution of securities through smart contracts.[35] The Blockchain Bill of Law IV of 24th July 2024 aims to expand Luxembourg's DLT legal framework by including equity securities alongside debt securities, allowing the fund industry to use DLT for managing shares, units, and registers. It introduces the role of a control agent as an alternative to the central account keeper, responsible for maintaining securities issuance accounts, verifying DLT consistency, and supervising the custody chain.[36] The law simplifies payment processes and the issuance of dematerialized securities, permits the direct crediting of securities to investor accounts, and allows for smart contract integration.

As such, Luxembourg does not regulate smart contracts used for forming and executing contractual securities. Mostly, the Luxembourg legal framework seems to focus on investment opportunities for clients rather than contractual opportunities for securities. They are the object of investments and can be used as collaterals, but they do not constitute the means to form nor execute a contractual agreement, and *a fortiori* a security. The different laws have expanded the scope where DLT can be used as an object of investment or collateral, it does not encompass the use of DLT as a mean form and execute traditional securities. Luxembourg has not yet legislated nor the CSSF have established guidelines for the use of DLT as a mean to form and execute securities.[37] However, such lack of regulation does equate to a legal void, as DLT used a mean to form and execute securities can be

35 Loi du 15 mars 2023 portant : modification de
la loi modifiée du 5 avril 1993 relative au secteur financier; la loi modifiée du 5 août 2005 sur les contrats de garantie financière; la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers et mise en œuvre du règlement (UE) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) n° 600/2014 et (UE) n° 909/2014 et la directive 2014/65/UE.

36 Projet de Loi n° 8425, portant modification : de la loi modifiée du 6 avril 2013 relative aux titres dématérialisés; de la loi modifiée du 5 avril 1993 relative au secteur financier; de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier.

37 CSSF, *Distributed ledger technologies and blockchain: technological risks and recommendations for the financial sector* (2022) 1–44, 4.

permitted, but it must be framed adequately pending a compliance with the technological nature of such endeavour as well as compliance with the principles of contract law.

Coupled with the innovative stance taken by Luxembourg on DLT, the formation and execution of securities through smart contracts remain tangible for the near future. This section has demonstrated that, while DLT and Blockchain have been considered by Luxembourgish law, it does so as an object rather than a mean to enforce obligations. Despite such an awareness, smart contracts as a mean to form and execute securities are not yet framed by law. In such a perspective, it is important to assess at what extent can securities rely on such technology and what their regulation would be.

II. Addressing challenges for establishing securities through smart contracts

As abovementioned, the formation and execution of securities relying on DLT imply a degree of automaticity and immutability that would ensure a certain degree of legal security. However, this also requires a relinquishment from the parties to the smart contract's execution. Thus, two main aspects present challenges for such prospect. On one hand, challenges due to the technological nature of the smart contract (A), on the other hand on the nature of securities (B).

A. Challenges stemming from the smart contract perspective.

As a technological tool, a smart contract brings several advantages for forming and executing securities. Although it requires a certain amount of digital assets established on the Blockchain, it could bring new means for financial institutions to enforce their securities. Due to its automation and immutability, legal certainty of the execution of the security would be prioritized. However, such perspective entails legal challenges regarding the establishment of DLT for this specific purpose. In order to secure the formation and execution of the security, several challenges need to be addressed, especially regarding the technical standards the smart contract needs to meet (1). Furthermore, the features of the smart contract, meaning the automation, delegation, and immutability, need to be addressed regarding under the context of securities (2).

1. From contractual clauses to computer code

The purpose behind the technical standards of the smart contract is to be able to form and execute the security as intended by the parties, as it lies at the core of its formation. Any derivation from such intent might strike the contract with the vice of disrespecting the will of the parties, hence leading to render the security clause void. This entails a dual approach.

Firstly, an intrinsic approach needs to be taken, meaning the one endorsed by the parties and the programmers. It entails that the Smart contract is properly encoded as to follow the will of the parties. The process of coding contractual clauses concerning collateral into smart contracts, particularly for financial securities or lending arrangements, involves ensuring that the intent of the parties regarding the collateral is translated accurately into code**.** The legal provisions governing the security, such as how and when it can be accessed, liquidated, or returned, must be accurately reflected in the smart contract. For instance, a smart contract needs to continuously monitor the value of the collateral, using price oracles, meaning trusted, appropriate, and relevant data feed that would automatically trigger liquidation if the collateral's value fell below the agreed threshold.[38] Oracles are a mean to obtain real-time, external data feeds about the value of the collateralized assets.[39] For example, if the collateral consists of financial instruments like stocks or bonds, the smart contract must integrate with oracles to fetch market data. Thus, they are indispensable for the proper execution of the security. However, parties might rely on different sources to assess the value of the collateral. Hence, they must agree on reliable price sources such as Bloomberg, Refinitiv, or cryptocurrency price oracles to feed real-time valuation data into the smart contract. Indeed, the smart contract should specify which data provider will serve as the single source of truth for collateral valuations. Moreover, legal contracts related to collateral can sometimes be open to interpretation of the creditor. For example, a clause might require the creditor to "*act in good faith*" or provide "*reasonable notice*" before liquidating the collateral.[40] This is challenging for the implementation of smart contract solution, for these terms are highly

38 Chanelle Duley, Leonardo Gambacorta, Rodney Garratt and Priscilla Koo Wilkens, 'The oracle problem and the future of DeFi' (2023) *BIS Bulletin* No 76, 1–7, 1.

39 ibid.

40 Philippe Ancel, *Contrats et obligations conventionnelles en droit luxembourgeois* (Larcier 2016) 15, 128, 143; Philippe Hoss and Patrick Santer, 'Le contrat fiduciaire en droit luxembourgeois' (Larcier 2003) *Études fiscales internationales* 781–856, 797.

subjective whereas the smart contract reasons in terms of quantitative and objective terms dependent on the programming it is subjected to.

However, one needs to distinguish such subjective terms from objective and quantitative solutions for adapting the contractual clause to the smart contract. For instance, measurable conditions such as margin requirements, collateral valuation on the relevant market could provide an adapted solution to avoid a subjective approach of the smart contract. This also entails that smart contracts used for securities purposes would not be adapted to all kind of securities, only ones that are able to be triggered with objective and quantitative event. Hence, for a smart contract to function properly, the terms related to collateral must be precise and quantifiable. This involves defining objective conditions that the smart contract can automatically monitor and enforce. If the collateral consists of assets like stocks, bonds, or cryptocurrencies, the smart contract must integrate oracles that provide up-to-date price feeds. Thus, the contract will need to define how often the collateral's value is checked and which source is considered authoritative. Clear thresholds need to be set for when collateral can be liquidated. For example, the smart contract could include a rule stating that if the value of the collateral falls below 70 % of the outstanding loan, the liquidation process is automatically initiated. Each clause related to collateral: its valuation, its liquidation and its substitution should be represented as a separate, modular function in the code.

Secondly, an extrinsic approach, ensuring that the smart contract works accordingly and is verifiable for auditing purposes. Formal verification can be used to technically verify that the smart contract code corresponds to the legal agreement. This ensures that the collateral management, valuation, substitution, or liquidation; is executed exactly as agreed upon by the parties. More than this 1st control verification, there needs to be a 2nd and 3rd control verification, to auditors and to courts in cases where the formation and execution are disputed by one of the parties. This requires an auditing procedure whose tasks is to ensure the technical standards of the smart contracts are upheld Ensuring that the smart contract code is auditable allows third parties and courts, in cases of legal dispute, to review whether the contract behaved as expected. This is especially important for disputes concerning collateral liquidation, where significant monetary value could be at stake. More than the program itself, it would also require a detailed documentation outlining how the smart contract's collateral terms were codified, and the original intent of the parties can serve as evidence in case of disputes.

2. The Automation, the immutability, and the delegation

Other notable challenges regarding the implementation of securities through smart contracts regard their intrinsic features, meaning their automation, immutability, and the delegation of its execution to a program.

Automation entails several challenges, especially regarding the complexity of securities' management. As previously mentioned, the value of collateral fluctuates particularly when dealing with market instruments, certain qualified as volatile such as certain types of crypto-assets. An oracle must constantly monitor market data to ensure that the collateral meets the agreed threshold. However, the value of some instruments can be volatile, and setting automated liquidation triggers can lead to premature or unwanted liquidations due to short-term market fluctuations without considering the long-term approach of certain instruments. In collateralized transactions, a margin call may be triggered automatically if the collateral falls below a certain percentage of the loan value.[41] However, there are challenges in automating complex margin management. For example, how should the contract handle partial liquidations or top-up requirements? These processes, traditionally managed by humans with room for negotiation, may be harder to automate and outsourced entirely. Black swan events, meaning unexpected market conditions concretized by liquidity shortages, market disruptions or market crashes can impact the collateral value leading to forced liquidation at an unwanted value for both parties.[42] Furthermore, if an oracle fails to deliver accurate data, the smart contract might fail to execute correctly or could initiate unintended actions such as triggering a liquidation at the wrong time. Human managers often have discretion in deciding how to handle situations such as minor breaches of collateral terms, giving parties time to top up collateral or negotiate. In contrast, a smart contract will automatically execute based on pre-programmed rules, potentially leading to outcomes that the parties would not have chosen if human discretion were involved. For example, the smart contract may immediately liquidate assets if a small margin call is missed, even if the default is temporary.

41 Committee on Payment and Settlement Systems, *Strengthening repo clearing and settlement arrangements* (Bank for International Settlements 2010) 1–65, 7.

42 Indrani Sengupta, 'An Exhaustive Study of the Black Swan Events in the Financial Markets' (2020) 10(2) *Journal of Management Sciences* 22–35, 22.

Securities agreements often evolve based on market conditions or business needs.[43] If the terms of the contract need to be modified, for instance adjusting collateral requirements in response to a change in market changes, one can take the path of renegotiation. However, with immutable smart contracts, once the code is deployed, changes are extremely difficult to implement. If the parties wish to amend the collateral terms, they will have to either deploy a new smart contract, which could be costly and time-consuming, or rely on off-chain agreements, which could undermine the trust and automation provided by the smart contract in the first place. If there is an error in the smart contract code, it cannot easily be fixed due to its immutability and could result in a failure to execute proper margin calls, or premature liquidation, which could have severe financial implications for the debtor.

Delegating key decisions related to collateral management to a smart contract can enhance efficiency but also introduces new risks. In traditional financial transactions, humans manage collateral with the ability to negotiate, delay, or adjust actions. When collateral management is delegated to a smart contract, parties lose the ability to exercise discretion or make subjective decisions. For example, if collateral values are volatile but likely to recover, a human might choose to wait before liquidating; a smart contract would proceed with liquidation according to its code, regardless of market context. Once authority is delegated to the smart contract, the contract will enforce collateral rules rigidly, without considering the context or relationship between the parties. This can lead to situations where a party's intent is not respected by the automation of the contract. Moreover, in some cases, collateral agreements involve multiple parties. Delegating collateral management to a smart contract requires careful coding of each party's rights and obligations. This adds significant complexity, especially when trying to automate decision-making that traditionally involved negotiation among parties. Most smart contracts do not have built-in dispute resolution mechanisms like traditional contracts entailing that once the collateral is liquidated there is no possibility to reverse the transaction unless the smart contract explicitly allows for it.

Furthermore, certain complex situations may require human judgment. For example, if the collateral's value is disputed or if there is a misunderstanding about the terms of the contract, human oversight is often

43 Albert Choi and George Triantis, 'Market Conditions and Contract design: Variation in Debt Contracting' (2013) 88(51) *New York University Law Review,* 51–61, 53.

necessary to resolve the issue, through mediation or court procedures. Delegating the entire process to a smart contract without room for human intervention can exacerbate conflicts when unexpected or nuanced situations arise. Moreover, as regulations evolve, the terms governing collateral in financial markets may need to be updated to reflect new legal requirement. Immutability makes it difficult to adjust smart contracts to remain compliant with such evolving legal frameworks. Ultimately, such a smart contract could result in non-compliance with adequate regulations, exposing the parties to legal or regulatory penalties and a voided contract. Immutability presents advantages, but also poses risks to the coherence of securities and the liquidation of the collateral, where subjective approaches can be privileged over an automated application of the contract. Through its technical standards, smart contracts present challenges for forming and executing securities. Furthermore, on a reversed approach, challenges stemming from the security law perspective also need to be addressed.

B. Challenges stemming from the security law perspective.

Not only under the challenges stemming from the Smart contract perspective, but the recourse to smart contracts to form and execute securities meet challenges from their legal framework. As such, there are challenges regarding the formation (1) and the execution (2) of contractual securities under Luxembourg law.

1. The formation of securities with a smart contract

The formation of smart contract containing contractual securities must be compliant with the general principles framing Luxembourg contracts. The main challenges lies on the consent of the parties to have recourse to such contract and at what extent the form it takes, an automated smart contract, is considered.

Thus, the question arises whether the form of the contract should be subject to the parties' consent. Traditionally, contracts are shaped documents outlining the obligations of both parties, with the execution of the security it contains carried out manually, notably at the initiative of the creditor. However, with the advent of smart contracts, the paradigm is shifting towards automation, where the software executes the terms of the contract

autonomously, without further involvement from the parties nor requiring such initiative from the creditor. In this context, where the form a contract has a significant impact on its execution, it is essential to consider the parties' consent extension to the smart contract form itself. Usually, the parties' consent focuses on the content of the contract, that is, what they agree upon and enshrined in its clauses.[44] If oral contract can be permitted, most of the time, they are under the written format. However, smart contracts are based on code and exist in a digital format. Thus, smart contracts introduce a new layer of complexity, as they automate execution once encoded, with no further input from the parties.[45] As a result, the form of the contract directly affects its execution and, consequently, has a direct impact on the parties themselves. Because of this direct influence, consent of the parties should be directed, more than the content of the contract, on the choice to resort to a smart contract as well. In this aspect, pursuant to article 1108, such consent must be clear, informed, and unequivocal.

In the context of smart contracts, the challenge is whether parties fully understand what they are agreeing to, particularly due to the technical complexity of how these contracts are executed. Thus, parties may consent to the terms, but might not fully comprehend the automated execution process, which may trigger legal issues if unforeseen consequences arise.

2. The execution of securities through a smart contract

Smart contracts are self-executing and operate based on predefined conditions encoded into the software. This creates issues with traditional concepts of contract performance and enforcement under Luxembourg law, which generally involves parties and possibly courts overseeing its performance. The automatic execution of smart contracts leaves little room for discretionary decision-making or renegotiation, which is a common feature in traditional contracts.

Indeed, the conditions encoded into the smart contract are fulfilled, the contract executes automatically, leaving no room for human intervention. This rigidity contrasts with traditional contract law, which allows for rene-

44 Pascale Dufour, *La théorie générale du contrat au prisme des travaux d'Axel Honneth* (Larcier 2023) 425.

45 Stuart D Levi and Alex B Lipton, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (2018) *Harvard Law School Forum on Corporate Governance* 1–9, 2.

gotiation or modification during performance. Under Luxembourg law, parties in traditional contracts can invoke mechanisms like good faith, unforeseen circumstances qualifying as force majeure allowing an alteration or suspension of the execution.[46] With smart contracts, such flexibility is limited or non-existent unless pre-programmed into the contract. The absence of discretion in the execution process means that smart contracts do not allow for the human judgment traditionally involved in contract performance.[47] If an unexpected situation arises that changes the context of the agreement, such as force majeure, the smart contract will still execute the terms as coded by the parties. This could lead to outcomes that neither party anticipated or desired. For instance, Luxembourg law recognizes the principle of good faith in contract execution, requiring parties to act fairly and to avoid any actions that would undermine the purpose of the contract and the security.[48] With smart contracts, the rigid and automated execution could challenge this principle. For instance, if circumstances arise that would typically require one party to act in good faith and delay performance, such as the delivery of goods under dangerous weather conditions, the smart contract will not have the capacity to adapt unless it was specifically programmed to do so. This drastically contrasts with the traditional approach of securities, where such events, despite being external to the contractual relationship, can be considered before resorting to its execution.[49] Relying on smart contracts requires such a step, that was not entirely considered in traditional execution, for it is overseen by humans, capable of identifying and interpreting such events.

In traditional contracts, if performance becomes impossible due to unforeseen events (such as force majeure), parties can suspend their obligations or terminate the contract. Smart contracts, however, lack this flexibility unless force majeure or similar contingencies are coded into them. Under Luxembourg law, a party might be legally justified in halting performance due to impossibility, but a smart contract would continue to execute regardless. This raises the question of how Luxembourg courts would handle disputes where the smart contract continues to enforce obligations even after they become legally impossible to fulfill.

46 Luxembourg Civil Code, articles 1134 and 1148

47 Loi du 5 août 2005 sur les contrats de garantie financière, article 11(1); article 13–1 (2)

48 Luxembourg Civil Code, article 1134

49 Delphine Gomes, Constantin Iscru and Azadeh Djazayeri, 'New Luxembourg Reorganization Law and Financial Collateral arrangements' (2024) *Insight Out* 28.

III. Regulatory pathways for enabling securities through smart contracts under Luxembourg law.

Although, while smart contracts are fundamentally considered immutable, parties may need to amend or update the contract while it is activated. However, it requires it to have clearly defined mechanisms for amendments, allowing the parties to make updates when mutually agreed upon. The contract should include clauses that enable updates to reflect changing circumstances, regulatory requirements, or the evolution of the parties' agreements. For certain securities or financial agreements, parties may wish to build governance mechanisms into the contract. These mechanisms allow for dispute resolution, amendments, or modifications to be carried out through a vote or mutual agreement of the involved parties. In this perspective, it is necessary to adopt principles allowing the drafting of securities through smart contracts (A), before addressing the requirements that should be addressed by Luxembourg's norms (B).

A. Drawing guidelines from the intersectionality of Smart contracts and securities

This article has highlighted the challenges stemming from forming and executing securities through smart contracts under Luxembourg law. This requires the setting up of principles regarding the formation of securities (1) and principles for executing them (2).

1. Guidelines for forming the securities with a smart contract.

To use a smart contract for the formation of the security entails challenges for the parties. However, these challenges can be overcome, especially while considering several principles by which the smart contract should be framed by.

Firstly, because it aims at forming a security and because of its nature as a contract, it is undoubtful that it would be bound by article 1108, regarding the principles of contract drafting. The consent of the parties to resort to a smart contract must be explicit and clear, for as it was demonstrated above, its form has direct and effective impact on its execution. Thus, despite what is commonly encountered in security law, not only the consent must be carried out regarding the contractual clauses of the security, but also on the

form of the contract. One could also generalize such approach to all smart contracts under Luxembourg law, since the form intrinsically impacts the execution of the contractual clauses.

Secondly, the smart contract must show upstream guarantees that the DLT it is relying on properly functions. These guarantees can be obtained through a technical notice given to the debtor gathering clear and precise documentations on how the smart contract works, what are the failsafe built inside the DLT and what is the extent of automaticity it relies on. For instance, what is the degree of human intervention allowed in this context, especially considering the challenges stemming from the market environment, force majeure or other external events that could influence the execution of the smart contract. These upstream guarantees are a conduit toward consent, and the clearer this technical information are, the better the consent would be.

The formation of the smart contract mainly regards upstream guarantees and the consent toward using the form of a smart contract. However, several more principles should be adopted in the context of the execution of the security, especially considering the coding and the triggering of the transfer of the collateral.

2. Guidelines for executing securities with a smart contract.

Smart contracts must be drafted in a manner that allow contingencies to address events like force majeure, otherwise, their rigid execution could cause unfair or uncoherent outcomes. The pathways for avoiding such outcomes to arise during the execution of the security.

Firstly, parties to a smart contract can attempt to resolve some of these challenges by coding specific contingencies into the contract itself during the formation phase. For instance, they could include provisions for recognizing and enforcing a force majeure event, impossibility of performance, or the need to relinquish the execution to a human oversight in certain situations.[50] Parties could code conditions that temporarily pause or terminate the contract execution if certain unexpected events occur, such as natural disaster, interruption of the market. This would mirror the traditional force majeure principle recognized under Luxembourg law further allowing human intervention if an unforeseen event arises, providing a layer of

50 Eric Tjong Tjin Tai, 'Force Majeure and Excuses in Smart Contracts' (2018) 26(6) *European Review of Private Law* 787–804, 799.

oversight over automated performance. Smart contracts should also rely on established oracle mechanisms, when external data feeds or third-party confirmations are required before executing certain key actions or to ensure that triggered events are appropriately recognized. The immutability of the smart contract thus calls for upstream and explicit encoding, to ensure the execution of the contract remains compliant with the general principles of contract law and the specificities of the security it is carrying**.** However, this requires a complex cooperation between lawyers and the encoders of the smart contract. This relationship is not yet defined under Luxembourg law; however, one could extrapolate from other regulations establishing an intersection of technologies and law. In such frameworks, the creditor relying on the smart contract needs to ensure that the development of such technology will ensure his compliance under the adequate rules of contractual relationship.

Secondly, a practical approach under Luxembourg law might lead to use hybrid smart contracts for the more complex securities, which combine traditional legal agreements with smart contract elements.[51] This would allow for greater flexibility by having certain parts of the contract governed by traditional rules intervention while automating less complex or mechanical aspects through smart contracts. Hybrid contracts allow parties to benefit from the efficiency of automation while retaining flexibility in areas that require human intervention or legal discretion. For example, if the loan is secured by cryptocurrencies, the smart contract automatically would transfer the cryptocurrencies to a multi-signature wallet controlled by both the creditor and the debtor. The debtor pledges cryptocurrency worth €500,000 as collateral. The smart contract automatically locks this collateral in a multi-signature wallet. The creditor disburses a €300,000 loan in the context of an over-collateralization, notably due to the volatility of the pledged asset. The debtor makes regular payments, which are automatically deducted from their account by the smart contract. Payments are recorded on the blockchain, and the smart contract updates the loan balance. Due to market fluctuations, the value of the cryptocurrency chosen as collateral falls to €250,000, triggering an automated margin call. The smart contract sends a notification to the debtor to provide additional collateral in order to match the original value. The debtor could contact the creditor and

51 Carlos Molina-Jimenez and Sandra Milena Felizia, 'On the Use of Smart Hybrid Contracts to Provide Flexibility in Algorithmic Governance' (2024) 6: e8 *Data & Policy Cambridge University Press* 1–11, 6.

requests more time to provide additional collateral. Thus, the creditor, using the hybrid contract's provisions, agrees to pause the liquidation process by activating the smart contract's kill switch allowing either party, or a neutral third party, to pause or halt the execution of the contract in certain circumstances Moreover, relying on more automaticity, a kill switch could be triggered by predefined events, such as one party notifying the other of a legal or technical issue. The smart contract would halt, and parties could address the matter through traditional legal channels before execution continues. After the borrower successfully repays the loan, the smart contract automatically releases the collateral back to the borrower. In case of default, if no agreement is reached, the smart contract automatically transfers the collateral to the lender according to the terms agreed upon in the traditional contract.

B. Regulatory perspectives under Luxembourg law

Due to the technical challenges associated with smart contract used for security purposes, one should consider an appropriate regulation. However, such regulation should take different paths in order to approach it adequately. Two levels can be considered. Firstly, a general and legal approach for ensuring a fundamental layer of principles applying to smart contracts used for security purposes. Secondly, a specific approach needs to be undertaken by the professionals when the drafting occurs,

Firstly, a further Blockchain law should open the recourse to DLT as a mean to form and execute security. This opening follows the legal logic that Luxembourg has established considering such technology and would also need to be accompanied with fundamental guarantees adequate for such smart contracts. This article highlighted the need to recourse to unavoidable features to ensure the coherence of the smart contract with security law. Among them, the recourse to an agreed oracle, upstream compliance with the general principles of contract law as stated in article 1108, and the technical recognition of contract execution principles, such as force majeure. What such legal regulation needs to consider, is the framing of principles needed for ensuring compliance between the general principles of contract law with smart contracts used for security purposes. Such an approach should also consider ensuring the parties have clearly established the triggering event and its dependence on an agreed oracle, to limit the risk of undue financial risk to the debtor.

Secondly, a more specific approach needs to be undertaken by the parties in order to fill the gap that would not be appropriate to address at the level of the law. This would mostly regard the choice of the appropriate security depending on the business relationship between the parties. It would be challenging for a law to address every technicality that the parties must have recourse to, given the freedom the parties should enjoy in drafting the smart contract. Nevertheless, these requirements should be addressed to offer technical safeguards. In this approach, compliance with the specific requirements of a specific security needs to be upheld by the parties foremost. They would need to ensure that the execution of the smart contract rigorously follows the requirements of the security they chose. Hence, such precise compliance at the technicality level mainly regards the securities enshrined in the law of 2005 for its requirements answer both formal and substance ones. In this phase, the legal requirements must be carefully implemented into technical standards by which the smart contract will abide. It is difficult to equate a general approach for this aspect, for it would be up to the parties to decide of the triggering event, the choice of the collateral, the terms of the security. What is crucial in this aspect, is to ensure that the will of the parties, and the execution of the security thereof, is ensured through the smart contract.

IV. Conclusion

While Smart contracts used for forming and executing securities can streamline the process of establishing and enforcing a security, its implementation can be challenging under Luxembourg law. Its features call for an upstream awareness from the creditor to answer both technical and legal requirements ensuring a compatibility with Luxembourg law. Moreover, while some securities can be more adapted for a full-fledged smart contract, the resort to hybrid ones should also be considered to avoid a full and unbeneficial automation of the contract leading to uncoherent outcomes. Creditors need to address what security would be adapted to either a smart contract or hybrid smart contract, the latest providing more room for human intervention than the first. The regulative perspective must spouse the flexibility offered by securities and the principles that should frame the formation and execution of smart contracts.

Creditors must also ensure of the opportunity of resorting to a smart contract, depending on the security they aim at integrating in its function-

ing. A coherence must occur during the drafting of the smart contract to ensure that it is adapted to the nature of the security and the business relationship with the debtor.