LETZBLOCK

SMART CONTRACTS
A LUXEMBOURG PERSPECTIVE

ASSESSING OPPORTUNITIES AND KEY LEGAL CHALLENGES

July 2021

FOREWORD

This paper has been prepared by the smart contract working group of LëtzBlock, the Luxembourg Blockchain & DLT Association.

LëtzBlock is Luxembourg's community hub for blockchain initiatives. Its main objective is to create a positive impact on the wider community by encouraging and supporting the development and adoption of blockchain and DLT-related ecosystems in Luxembourg.

The Luxembourg ecosystem is thriving, with many initiatives and projects already active. LëtzBlock brings them together via a common platform and environment allowing existing actors to connect and facilitating the transformation of the Luxembourg DLT and Blockchain landscape.

The LëtzBlock smart contract working group was headed by:

Anne BAUDOIN, docteur en droit and Avocat à la Cour au Barreau de Luxembourg (Etude Korving, Luxembourg).

Members of LëtzBlock Smart Contract Working Group actively involved in this project were:

➢ Monique BACHNER, Independent Director, Board Advisor, and Solicitor (England & Wales);

➢ Boika DELEVA, Avocat à la Cour au Barreau de Luxembourg, Clifford Chance, Luxembourg;

➢ Anthony FAVIER, Avocat aux Barreaux de Paris et de Luxembourg, Etude Elvinger Hoss Prussen, Luxembourg;

➢ Olivier MARQUAIS, Avocat aux Barreaux de New-York, Ontario, Paris, Québec et Luxembourg, Loyens & Loeff, Luxembourg;

➢ Vincent-Emmanuel MATHON, Engineer and Doctor of philosophy, Luxembourg;

➢ Yohan MAURIN, Blockchain Developer, PWC, Luxembourg; and

➢ Roger TAFOTIE, Entrepreneur and Lecturer, The Blockchain Academy.

The LëtzBlock Smart Contract Working Group (the "SC Working Group") was set up in early 2020 at the initiative of the LëtzBlock board of directors. The SC

Working Group's road map was to raise awareness on the development of smart contracting and to identify the legal challenges that could be associated thereto considering Luxembourg law and regulations. A multi-disciplinary approach was favoured and therefore the SC Working Group was not solely composed of lawyers: it included a philosopher and engineer, as well as a blockchain developer.

During the first phase of the project, the SC Working Group focused on the concept of "smart contract". Once a common definition was agreed upon and the potential use cases of smart contracts explored, the SC Working Group discussed when and how smart contracts could fit within the realm of Luxembourg law. The main aim here was to identify the potential areas of legal uncertainty and associated challenges and to seek Luxembourg stakeholders views.

The outcome of these various discussions was the Survey that was launched on 22 September 2020 and ended on 13 December 2020. This Survey was publicised not only by LëtzBlock using its social media and website, but also through, or via other Luxembourg professional associations.

The second phase of the project was the drafting of the present white paper (the "White Paper") which took place between September 2020 and mi-April 2021. This White Paper summarises the outcome of the work and some key findings of the Survey[1]. It does not reflect or mention any Luxembourg or European publications relating to smart contracts taking place after mid-April 2021.

Caveats: Please note that this White Paper does not constitute legal advice. It is intended to share thoughts and to provide suggestions on matters related to smart contracts and some of their legal consequences. Views expressed are those of the active members of the SC Working Group and do not reflect the view of their employers or of any organization.

[1] The Survey can be accessed here.

Acronyms

AML	Anti-Money Laundering
CNIL	Commission nationale de l'informatique et des libertés (French data protection agency)
CNPD	Commission nationale pour la protection des données (Luxembourg data protection agency)
DLT	Distributed Ledger Technology
eIDAS	Electronic identification and trust services for electronic transactions in the internal market (EU Regulation N°910/2014)
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
ICO	UK Information Commissioner's Office
ILNAS	*Institut Luxembourgeois de normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (Luxembourg agency for standardization and quality of products and services)
ISAE	International Standards for Assurance Engagements
ISO	International Organization for Standardization
IT	Information Technology
IP	Intellectual Property
WIPO	World Intellectual Property Organization

Executive summary

The potential of smart contracts has not yet been realised, with their possible use and applications in various industries and socio-economic areas. It appears challenging to launch and scale products and services based on smart contracts because many policy and legal and regulatory environments have not genuinely been enabled yet.

The aim of this White Paper is to raise, from a Luxembourg perspective, legal and regulatory challenges stemming from the adoption of smart contracts and to provide a useful tool for the legislator, regulators and all other stakeholders to engage more effectively. It elaborates commonly discussed and challenging issues or positions by researchers and practitioners of smart contracts, backed up by a survey.

Agreeing on the features and on a definition of "smart contracts" is a prerequisite for assessing key legal and regulatory challenges that a broader adoption of smart contracts may raise from a Luxembourg legal perspective. Such a prerequisite is also critical for discussing new horizons that smart contracts could open not only from a socio-economic viewpoint, but also from a political or philosophical standpoint.

This White Paper aims therefore to propose a definition that could reconcile the technical concept of smart contracts, with the legal concept of contract, while being sufficiently large to leave the door open to new use cases. Building bridges between "legal" contracts and smart contracts appeared as a need to be addressed from a legal perspective, and from a technical perspective.

As Luxembourg law may be applicable to smart contracts considering their potential legal consequences, some key legal challenges the use of smart contracts may raise from a Luxembourg legal viewpoint have been examined, the initial one being the stage of a contract lifecycle where smart contracts may be used.

Finally, the broader adoption of smart contracts may open the doors to challenges other than the legal ones with respect to current Luxembourg legislation briefly addressed in this White Paper. Readers will also find some food for thought in this respect.

Introduction

Contracting

In our daily life, a contract is mainly the practical implementation of the principles of freedom of trade and industry and, in particular, of the principle of contractual freedom, we, as Europeans and Luxembourgers, benefit from.

A contract is a legally binding agreement governing the parties' (economic) relationship and setting out their respective courses of action.

In common law and civil law jurisdictions, most contracts do not have to be in written form in order to be valid, and nearly all agreements in our daily lives are verbal. Recording on paper the components of the parties' understanding remains, however, good business practice and serves as the footprint (*instrumentum*) of the agreement, a reminder of the parties' obligations as well as an evidence in case of litigation or dispute.

In Luxembourg, like in many other civil law jurisdictions, the Civil Code (*Code civil*) itself is a consequence of a more general contract, namely the so-called social contract (*contrat social*), binding each individual living in the same nation within a society as a whole.

The aim of this social contract (as envisioned by Jean-Jacques Rousseau in his book *Du Contrat social*[2]) is to safeguard freedom of all. Specifically, contracts originated as shared "islands of predictability" intended to mitigate the uncertainty for the human community by reducing conflict, frustration, oppression and anger and, therefore, to produce trust, cooperation, cohesion and adaptation when humans are facing the uncertainty that is inherent to their lives. All those rules are either unwritten or foreseen in the Constitution of the Grand-Duchy of Luxembourg, especially its Chapter II relating to public freedoms and fundamental rights.

The Civil Code provides the legal framework for contracting by explicitly setting out the conditions of contract formation and related effects, enforceability, termination, rules of interpretation, content, types, resulting liability and other particularities of contracts, as guided by core principles, such as party autonomy and good faith.

[2] *Du Contrat Social,* J.J Rousseau, first published in Amsterdam, 1762.

Smart contracting

Smart contracts, however, do not necessarily fall within the framework defined by the Civil Code and may further not fall within the common acceptance of what a contract is, and what its traditional consequences are.

Reaching a consensus on the definition of smart contracts may even be challenging since different distributed ledger databases (i.e. blockchains[3]) may offer different smart contracting capabilities and, more generally, because the terms ("smart" and "contract") may relate to different concepts depending on our respective domain of expertise.

The traditional features of smart contracts include reliance on computer code allowing self-execution upon the occurrence of predetermined (e.g. real world) events. Thus, they imply a degree of automation which may be used to remind contracting parties of the actions which they must undertake. Smart contracts can even perform these actions on their own (i.e. without human intervention) when the relevant conditions are met – on an "if this – then that" basis, provided that they are appropriately triggered.

To the extent that contracting parties' actions or decisions are sufficiently operational and clear to be expressed in a binary language[4], they may be represented in coded or programmable language and processed by algorithms[5], thus achieving an unprecedented degree of certainty.

Going further down the road, most decisions could be processed through algorithms in the future, provided that they can be translated into a process which itself can then be coded. Considering current technological developments and improved knowledge of human decision-making processes, algorithms could even trigger actions leading parties to the "best possible outcome" for all of them, or to

[3] A definition of the terms "Blockchain" may be found in Appendix 2 - The Glossary.

[4] A binary language or code is a mathematical language relying on a base-2 number system and used by computers. More details can be found under the definition of binary code of the Britannica Encyclopaedia (https://www.britannica.com/technology/binary-code, accessed on 5 January 2021).

[5] An algorithm is defined in the Merriam-Webster dictionary as "*a procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation* (see https://www.merriam-webster.com/dictionary/algorithm, accessed on 5 January 2021).

an optimum according to John Nash's Bargaining theories[6], reducing human implication in the decision-making process. This would then fulfil Leibniz's dream: "we disagree, let's calculate."[7] Would this mean that smart contracts could allow abandoning the human world of legally binding promises and substitute it instead with the positivist calculations of automated machine processes? Philosophers as well as any person concerned by the future of our society may wish to keep this likely effect in mind.

As of today, smart contracting does not aim to exclude or even replace traditional contracting, and *vice versa*, as both smart contracts and traditional contracts coexist and reliance on human factors remain important in both cases. Some challenges, which we seek to address in this publication, relate to how these two models may interact and be combined under Luxembourg law.

However, irrespective of whether and how smart contracts fit in the realm of Luxembourg contract law, reducing human involvement in contracting raises a number of questions including, in particular, whether automation is always in the best interest of contracting parties, whether it necessarily achieves the best possible outcome and what are the most appropriate provisions for automation.

In our opinion, while ousting human beings from the contracting process may, in selected cases, be technically feasible, this may not be desirable for any legal agreement regardless of the state of evolution of the technology. Indeed, irrespective of how much trust one may place in algorithms, considering the contracting process exclusively through a binary lens is bound to oversimplify legal concepts and norms which have taken centuries (if not millennia) to develop and crystallise into their current form. Thus, a degree of human trust and oversight is – and will likely continue to be – needed.

This being said, contracting parties will, at least to some extent, have to trust the computer code to trigger certain actions (even as seemingly insignificant as a reminder), if they wish to benefit from the advantages of this technology, despite the fact that it is prone to unavoidable early days hiccups and glitches. This can be compared to the trust we need to have in computer programs. A collaborative mindset between the various stakeholders will remain necessary at this early stage

[6] See *The Bargaining Problem*, J. Nash, *Econometrica,* Volume 18, issue 2 (Apr. 1950), 155-162.

[7] The original quote by Leibniz is in Latin ("*calculemus*") and can notably be found in his essay *De arte characteristica ad perficiendas scientas ratione nitentes.*

of (legal) smart contracting to facilitate trust in the algorithms. Agreeing on some contractual measures would also give appropriate confidence that a party will not exploit any technological malfunctions, such as coding errors.

The LëtzBlock SC Working Group has not performed an in-depth legal, technological or economic analysis of smart contracts and their use. The SC Working Group has rather focused on specific points, and in particular legal challenges, which it deemed critical to address in order to support the adoption of smart contracts in Luxembourg. It appears from the various discussions of the SC Working Group that existing legal solutions relating to the Internet, content hosting or online agreements may already provide the appropriate foundations to analyse and solve legal issues that may arise from the increased use of smart contracts and the use of the underlying blockchain (or DLT) technology. Discussions regarding the various novel legal challenges arising out of the use of DLT based smart contracts require us to reconsider the issue of trust that currently underlines contract law and the role that automation, artificial intelligence and algorithms may take in this respect.

1. What is a Smart Contract?

As of today, there is no commonly recognised definition of what a "**smart contract**" is, from an EU or Luxembourg viewpoint. Common features can be found in most of the definitions currently available in legal and technical literature. One's professional background, technical language and expertise will determine which features to focus on. It should however be kept in mind that the meaning of a word can vary from a professional sector to another. For example, the term "agent" will not have the same meaning for a computer scientist and for a lawyer.

The SC Working Group considered necessary to share its understanding of smart contracts and their features in order to contribute knowledge and expertise, from a legal, academic, technological and philosophical perspective to assist other experts involved in the development, execution or resolution of issues associated with smart contracts and facilitate their implementation on an *ad hoc* basis or their adoption on a larger scale.

This chapter aims to define smart contracts from a technical viewpoint and address the possible links between smart contracts and traditional contracts in accordance with Luxembourg legal principles, norms and concepts. The authors here seek to bridge the gap between the technologists (who tend to focus on computer code) and the legal community (which rather focuses on legal and contractual provisions).

We will then introduce the concept of the "hash" given the importance and various uses of this function in the deployment of smart contracts.

Finally, we will review past or current smart contracts use cases as well as the economics of smart contracts to support their development and practical implementation in the future.

1.1 Smart contracts: a technical concept first and foremost

The concept of "smart contracts" originates from the world of computer science, which tends to provide its own definitions of terms commonly perceived as otherwise having an entirely distinct meaning in everyday use. For example, the acronym "S.M.A.R.T." generally refers to "Self Monitoring Analysis and Reporting Technology". Further, we are now witnessing a trend towards more connectivity using, in particular, the Internet of Things, giving rise to new concepts such as "Smart Cities" or "Smart Computing".

Thus, the combination of the terms "smart" and "contracts" should not come as a surprise. However, by reason of the usual acceptance of the term "smart" and the legal meaning of the term "contract", a widely accepted difficulty is that "smart contracts" often are neither smart, nor contracts.

The first definition of "smart contract" was provided by Nick Szabo[8], a cryptographer, computer scientist and legal scholar, who defined it in his 1997 seminal work as "a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs." The practical example given by Szabo was the use of a vending machine, while however stressing that the smart contract use cases go beyond this particular case and placing the focus on the execution of the contractual terms, rather than on the conclusion of a legally binding agreement (which was deemed to already exist).

Subsequent definitions focused more on the computerised transaction protocols implemented by using distributed ledgers or on the self-execution mechanism embedded in smart contracts. Amongst the many definitions of a smart contract provided by the legal community, the authors agree that the most appropriate non-technical definition to level the playing field for the general public is "an agreement whose execution is automated. This automatic execution is often effected through a computer running code that has translated legal prose into an executable program. This program has control over the physical or digital objects needed to effect execution. Examples are a car that has a program installed to prevent ignition if the terms of a debt contract are not met or banking software that automatically transfers money if certain conditions are met. A smart contract does not rely on the state for enforcement, but is a way for contracting parties to ensure performance."[9]

Vitalik Buterin (Ethereum co-founder) even came to regret the use of the term "smart contract" in a tweet he posted on Twitter on October 13, 2018: "To be clear, at this point I quite regret adopting the term "smart contracts''. I should have called them something more boring and technical, perhaps something like "persistent scripts''.[10]

Since the inception of this project, and especially since the finalisation of the Survey, new definitions of smart contracts have been proposed. For example, in

[8] Nick Szabo, the Idea of Smart contracts, 1997, https://nakamotoinstitute.org/the-idea-of-smart-contracts/, accessed on 13/05/2020.

[9] Max Raskin, The law and legality of smart contract, Georgetown Law Technology Review 305 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166.

[10] https://bitcoinist.com/vitalik-buterin-ethereum-regret-smart-contracts/ , accessed on 13 May 2020.

a Staff Working Document published on 24 September 2020, the European Commission has given the following definition: "A smart contract is a piece of software that runs directly on DLT and can replicate a given contract's terms. It effectively implements the terms of an agreement (e.g. payment terms and conditions) into computational material to automate the execution of contractual obligations"[11]. However, no such definition was officially embedded in the draft regulation proposed by the European Commission as part of the current EU digital finance package, despite its aims to propose "a comprehensive pro-innovation legal framework in the areas of digital assets and smart contracts"[12]. A reason might be that the scope of the proposed pieces of legislation does not intend to regulate smart contracting itself.

Another example is ISO which provided in July 2020 the definitions of a number of terms and concepts relating to blockchain and DLT, and in particular smart contracts. The latter are defined as "computer programs stored in a DLT system herein the outcome of any execution of the program is recorded on the distributed ledger. A smart contract can represent terms in a contract and create a legally enforceable obligation under the legislation of an applicable jurisdiction."[13] The authors anticipate that the ISO definition may become, over time, the standard technical definition.

A last example comes from a recent law of the State of Wyoming Law relating to decentralized autonomous organizations ("DAO"), effective on July 1, 2021, for which "Smart contract means an automated transaction, as defined in W.S. 40-21-102(a)(ii), or any substantially similar analogue, which is comprised of code, script or programming language that executes the terms of an agreement and which may include taking custody of and transferring an asset, administrating membership interest votes with respect to a decentralized autonomous organization or issuing executable instructions for these actions, based on the occurrence or non-occurrence of specified conditions"[14].

In our view, determining and agreeing on the key characteristics of smart contracts is critical to promote a shared understanding of the concept. To this effect, the SC Working Group considers that the European Commission Staff

[11] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, SWD/2020/201 final (page 6); https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0201, accessed on 6 January 2021.

[12] https://ec.europa.eu/digital-single-market/en/blockchain-technologies, accessed on 6 January 2021 and https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain, accessed on 24 March 2021.

[13] International standard ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en, accessed on 8 January 2021.

[14] See https://www.wyoleg.gov/2021/Introduced/SF0038.pdf, accessed on 12 April 2021.

Working Document and the International standard ISO 22739:2020, on the one hand, and previously mentioned definitions, on the other hand, are good starting points. The following generally agreed characteristics of smart contracts stem from these definitions:

- Smart contracts are deterministic pieces of computer code following Boolean logic;
- They are normally supported by blockchain technology (or more generally by DLT), but can also be deployed using cloud technology;
- If supported by a public blockchain, smart contracts will be more transparent and reliable in a third-party trust-less environment thanks to their reliance on a consensus mechanism and a decentralised control of the distributed ledger. In any case, smart contracts are supported by cryptographic encryption tool;
- The script underlying a smart contract is self-executing and self-enforceable (i.e. once the underlying code is final and running, no intervention of a third party is required for its execution);
- They can replicate certain specific contractual terms and allow automated execution of certain specific contractual obligations; and
- Smart contracts benefit from the immutability feature of the distributed ledger supporting them.

The key technical characteristics of smart contracts identified in the various definitions, doctrinal contributions and technical writings, shall serve as the basis upon which the legal community assesses smart contracts as a technological tool from a legal perspective. Their legal ramifications shall be assessed separately under each relevant applicable legal regime. The focus of this White Paper is to carry out such assessment under Luxembourg law.

1.2 Relationship between smart contracts and legal contracts

According to the majority of the respondents to the Survey (57,89%), smart contracts can qualify as contracts within the legal meaning of this term (31,58% opting for "may be" as an answer). However, only 45,45% of the respondents believe they can qualify as electronic private deeds within the meaning of Article 1322-2 of Luxembourg Civil Code (other respondents opting for a "may be" answer). Agreeing on the meaning of these legal terms is necessary to clarify possible interactions between smart contracts and traditional contracts in a legal sense.

From a legal perspective, a legally binding agreement - or a "contract" - can be concluded, documented, executed or even enforced with the support of traditional means (such as, a written or oral agreement, execution requiring human action, and enforcement through a court decision), but also within or by virtue of digital tools, including algorithms, and by using various supports to store and evidence their content or facilitate their execution (such as DLT, notably by automation of execution or automatic data feed). These various options can also be combined, which is actually the case in practice, as further detailed below in the section on smart contract use cases. For instance, automation may take place at the level of the performance of a contract, especially when digital assets are involved. Automation can even occur at the level of the enforcement, in cases where smart contracts are designed to settle a claim.

This flexibility derives from the general principle of contractual freedom under Luxembourg law. In particular, it is not legally required that terms and conditions of a legally binding agreement must be embedded in a single document. Rather, terms and conditions generally constitute a separate piece of contractual documentation which may be amended over time and may further be composed of various connected agreements. In addition, in the absence of specific legal provision, parties to an agreement are free to agree on the most suitable way to execute their respective obligations.

According to some blockchain authors[15] and, as acknowledged by certain respondents to the Survey, smart contracts should neither fall within the scope of the law, nor trigger litigation, because they are only pieces of code. However, smart contracts, like any IT programs, applications or computerised scripts, can affect human activities, directly or indirectly, and any human activity is subject to certain legal and regulatory boundaries. The fact that neither Luxembourg nor EU law addresses the specificities of smart contracts[16], or clarifies when they can fall within the scope of the (contract) law, should not be seen as a valid argument to conclude that smart contracts or more generally algorithmic contracts are outside of the scope of applicable laws and regulations.

Moreover, a smart contract may certainly qualify as a digital document - as defined in the eIDAS Regulation (Article 3) or in the Article 1322-2 of Luxembourg Civil Code -. Therefore denying legal effect to smart contracts or rejecting their use as evidence of the rights and obligations of contractual parties simply because of their electronic form would not be appropriate. Such interpretation would, *inter alia*, not be in line with the provisions of Article 46 of the eIDAS Regulation. The legal effect of a smart contract will simply differ depending on the actions triggered by its execution as well as on the relevant local laws and regulations. For this purpose, it is fundamental to be able to determine the legal framework (including applicable law and competent jurisdiction) relevant for smart contracts. This question may at first be challenging, however one should not forget that this was also the case in the early age of the Internet.

Deciding on legal issues that may arise from the use of smart contracts will ultimately remain vested with the courts and tribunals. In case of a dispute, and in the absence of alternative means of dispute resolution (including automated means of dispute resolution), the courts chosen by both parties will in principle be competent to interpret the application of existing laws and regulations to the use of smart contracts[17]. The reason why courts may ultimately be involved in the legal and technological debate over smart contracts is that European countries,

[15] Alexander Savelyev, Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law (December 14, 2016). Higher School of Economics Research Paper No. WP BRP 71/LAW/2016 Available at SSRN: https://ssrn.com/abstract=2885241 or http://dx.doi.org/10.2139/ssrn.2885241.

[16] Luxembourg has however amended some sectoral laws (Luxembourg Act of 6 April 2013 on dematerialised securities as well as Luxembourg Act of 1st August 2001 concerning the circulation of securities) to allow the use of blockchain and DLT with respect to securities.

[17] See e.g. Darcy W. E. Allen, Aaron M. Lane, Marta Poblet, "The governance of Blockchain dispute resolution", Harvard Negotiation Law Review, vol. 25, pp. 75-101, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3334674 accessed on 28 January 2021; Amy J. Schmitz and Colin Rule, "Online Dispute Resolution for Smart Contracts (June 26, 2019), in 2019 Journal of Dispute Resolution 103, University of Missouri School of Law Legal Studies Research Paper No. 2019-11, Available at SSRN: https://ssrn.com/abstract=3410450; Ibrahim Shehata, "Smart contracts and International Arbitration", available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290026 accessed on 29 January 2021.

such as Luxembourg[18], prohibit the denial of justice. Consequently, a party to a smart contract can always introduce a legal action before a court, in compliance with the laws and regulations on international competence of jurisdiction and the law applicable to the legal issues brought to the court's attention. The generally accepted principle of neutrality of the law with regards to new technologies should then apply.

Characterisation will help determine applicable laws and regulations as well as competent jurisdictions. However, it will require a clear understanding of the distinctive technical and – where relevant – legal features of a smart contract and when it could qualify as a contract within the meaning of the Luxembourg Civil Code.

Although, from a legal perspective, nothing prevents a smart contract (as understood from a technical viewpoint) to qualify as a contract (within the meaning of the Luxembourg Civil Code), current smart contracts are first and foremost used as a means of execution for legally binding agreements. They are therefore governed by the terms of such agreements, as evidenced through some of the use cases discussed further below.

Smart contracts are thus mainly computerised artefacts aimed at being implemented into the traditional contractual framework and, more generally, in the network of legal relationships existing in interconnected legal agreements or contractual chains.

The main issue with computerised and automated systems is their manifold diversity. In order to characterise them under the existing legal framework, there must be a common ground to step onto, a *Code civil* or Common Law of the algorithms.

In order to come up with a definition that takes into account both the technical nature of smart contracts as well as their potential legal implications, the SC Working Group also examined the definitions contained in the laws or bills of law of some jurisdictions, such as the State of Illinois[19] or the State of Arizona[20] in the U.S. In the end, these definitions were however not retained, as they were considered as either not being broad enough to capture all use cases or being

[18] Luxembourg Civil Code, Article 4.

[19] http://www.ilga.gov/legislation/publicacts/101/101-0514.htm (accessed on 14/05/2020): *"Smart contract" means a contract stored as an electronic record which is verified by the use of a blockchain.*

[20] https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf: *"SMART CONTRACT" MEANS AN EVENT-DRIVEN PROGRAM, WITH STATE, THAT RUNS ON A DISTRIBUTED, DECENTRALIZED, SHARED AND REPLICATED LEDGER AND THAT CAN TAKE CUSTODY OVER AND INSTRUCT TRANSFER OF ASSETS ON THAT LEDGER.*

limited to the legal definition of a contract (thus not taking into account the technical features of smart contracts).

From a Luxembourg legal perspective, the term "contract" means "an agreement by which one or several persons obligate themselves towards one or several others to give, to do, or not to do something." (Article 1101 of Luxembourg Civil Code). Smart contracts will thus not necessarily qualify as a contract or even as legal provisions of a contract: They may not fulfil the legal requirements for such a qualification.

As a result of the review of various legal or technical definitions, the SC Working Group initially retained the following definition which was also provided in the Survey for respondents to comment:

A smart contract is a computerised transaction protocol between two or more parties. It may be self-executing. It can qualify as a contract within the meaning of Luxembourg Civil Code if the relevant criteria of Articles 1101 and 1108 mainly are met.

Among the 26 respondents to this question, 16 agreed with this definition, 6 agreed partially and 4 disagreed. The main reasons invoked for disagreeing with the proposed definition were, on one side, the existence of the ISO definition published shortly after the finalisation of the Survey and, on the other side, the fact that smart contracts "are not smart and they are not contract[s]". Respondents who partially agreed with the proposed definition recommended some improvements. These included notably the use of a term broader than the term "computerised" to capture future technological solutions, or the removal of the references to the Luxembourg Civil Code, which would ensure a more generic and simpler definition than the one originally suggested.

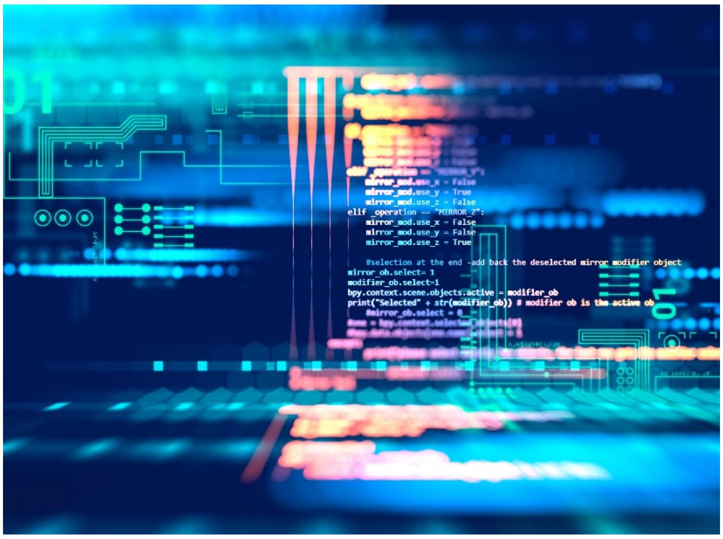
As a result, the following definition of "smart contract" was finally retained for the purpose of this White Paper, because it bridges the gap between the technological concept of "smart contract" and the potential Luxembourg law implications associated therewith:

> *A smart contract is an automated transaction protocol between two or more parties. It may be self-executing. It can qualify as a contract within the meaning of Luxembourg Civil Code if the relevant criteria provided in this Code (mainly in its articles 1101 and 1108) are met.*

Adopting a common definition of smart contracts would not only help with their legal characterisation, but also foster enhanced understanding of and trust into the technology, thus facilitating a broader adoption of smart contracts in our day-to-day contractual relationships.

1.3 Here comes the hash!

Proper use of hash functions is critical in the blockchain and smart contracts and can serve various purposes as discussed hereafter. As a result, providing a brief introduction of the hash function is necessary.



A hash function can be defined as "a function that converts one value to another. Hashing data is a common practice in computer science and is used for several different purposes. [...] Hashing is a natural fit for cryptography because it masks the original data with another value. A hash function can be used to generate a value that can only be decoded by looking up the value from a hash table. The table may be an array, database, or other data structure. A good cryptographic hash function is non-invertible, meaning it cannot be reverse engineered."[21]

The output of a hash function is generally referred to as a hash, also called a hash value. It is a bit string of fixed size, which may vary depending on the hash function used to generate the hash value[22].

There is no single type of hash function. Depending on its features, the hash function can be used for various purposes, including, among others, the following:

- To index documents stored in a database (such as a library database or a blockchain): In such case a different hash will be generated by a hash function depending on the digital content of the document;
- To compare documents without opening them, but performing a word-by-word comparison, and to determine if they are identical or not, relying for this purpose on the calculated hash values of the files. The hash value will be identical if the documents are word by word the same and if the same hash function is used to generate the hash;
- To identify the sender of a message and to ensure the integrity of such message: Identifiers of the sender are linked to a unique hash

[21] https://techterms.com/definition/hash (accessed on 18.06.2020) or on Code magazine (https://www.codemag.com/Article/1805061/Understanding-Blockchain-A-Beginners-Guide-to-Ethereum-Smart-Contract-Programming, accessed on 18.06.2020) among other sources.

[22] Please refer to Appendix 1 for a hash example.

known as the "public key" which can be deemed to represent them; or

- To link data blocks together in a blockchain/DLT, each block having its own hash as identifier and such hash being linked to the hash of the previous block (block hash).

In summary, it is important to keep in mind that any digital document may be converted into a bit string (numbers and letters) using the hash function. The hash allocated to the document would serve as its unique identifier.

1.4 Smart contracts use cases

There are numerous applications of smart contracts discussed in the legal and technological literature, covering a variety of different areas all the way from the financial industry or the insurance sector to the health, the logistic, art or video game sectors. While most of the successfully implemented practical use cases involving smart contracts are focused on improving the efficiency of the financial markets, the potential development of solutions using smart contracts is much broader.

Some of the use case applications in the banking and financial sector, which also leverage on the advantages offered by DLT, include the streamlining and automation of certain processes and transaction steps in financial transactions. For example, smart contracts can allow the quasi-instantaneous settlement of the obligations[23] arising under securities financing and repurchase transactions and other financial transactions once these trades have been agreed by the trading counterparties[24], as well as the possibility for real-time valuation of securities and collateral positions allowing for real-time exposure monitoring, thus decreasing

[23] https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf.

[24] Ream, J., Chu, Y., Schatsky, D. (2016). Upgrading blockchains: Smart contract use cases in industry. [Blog] Deloitte Insights, https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/using-blockchain-forsmart-contracts.html. Chamber of Digital Commerce, Smart contracts: 12 Use Cases for Business and Beyond, December 2016, https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf (accessed on 14/05/2020).

financial risks. The automation of the end-to-end lifecycle of securities, comprising the issuance and holding of securities directly on the DLT as well as their trading and settlement improves efficiency and reduces or completely removes certain operational and counterparty credit risks. The Luxembourg legal framework already caters for the possibility to issue dematerialised securities on the DLT[25] and allows custodians to hold securities accounts by virtue of DLT[26] and effect related securities transfers, thus permitting the successful deployment of digital solutions using smart contracts on DLT platforms[27].

Payment transactions are a further area where the implementation of smart contracts offers considerable benefits and efficiencies. For instance, the application of smart contracts in coupon payments, insurance premiums, automatic indemnification of damages in straightforward indemnification processes in the insurance sector[28] or generally any other type of periodical or pre-established payment operations decrease the risk of errors and reduce costs by eliminating the need for manual instructions and intervention. Settlement of payment transactions using smart contracts further improves transactional data integrity and decreases the risk of settlement failures.

The use of smart contracts crosses the borders of dematerialised assets and allows for an automatic and instantaneous transfer of rights in almost any asset which may be represented on the DLT by virtue of tokenization, thus improving the liquidity of highly illiquid assets, such as real estate.

The creation of a digital identity of goods for the purposes of reducing counterfeits and a digital identity of persons to support and facilitate identification and digital onboarding and transacting, while at the same time ensuring compliance with laws and regulations applicable in the fight against terrorism and money laundering, is

[25] Article 1*bis* of the Luxembourg amended Act of 6 April 2013 on dematerialised securities.

[26] Article 18*bis* of the Luxembourg amended Act of 1st August 2001 concerning the circulation of securities.

[27] https://www.infinance.lu/actualites/lgx-supports-idbs-green-bond-transparency-platform (accessed on 17 February 2021).

[28] https://www.artificiallawyer.com/2020/10/08/axa-scraps-fizzy-insurance-smart-contract-but-still-interested-in-the-tech/; Additionally, automated loss assessment for smallholder farmers pioneered by the Luxembourg-based start-up Ibisa Network: https://ibisa.network/.

a further example of use cases which are currently being explored both by private and public players.

Smart contracts are also used by beneficiaries or owners of IP rights to better protect their financial rights. In the music industry for instance, a blockchain start-up currently used to allows artists to sell music directly to fans via smart contracts (using Ethereum) that automatically split payments with collaborators.[29] Smart contracts and blockchain are even now used by artists or in the video game industry thanks to the use of non-fungible tokens or NFT[30].

The management of the supply chain is yet another area where use cases have been contemplated and even developed during the past few years to streamline and digitalise relevant information that needs to be shared among market players as well as to enhance tracing of the assets across the various stages of the supply chain and mitigate associated risks.[31] Out of the 7 international projects selected for the Luxembourg Blockchain Lab end of 2020, two of them were related to supply chain management[32].

It should however be noted that some of the projects launched in this respect were terminated, often due to a lack of sufficient economic benefits or market interest to offset the technological costs for their development in a foreseeable future[33]. This should however not preclude market players and professionals generally to choose smart contracts for modernising and streamlining operational processes and events.

1.5 Some economics of smart contracts

Similarly to other technological developments such as the Internet, music or videos streaming services or cloud-supported applications, the increased use of smart contracts and the successful implementation of new use cases will depend

[29] For details, see: https://ujomusic.com/. More generally on Blockchain/DLT and the music industry: Ignacio De Leon and Ravi Gupta, "The impact of digital innovation and blockchain on the music industry", Inter-American Development Bank, Discussion paper n° IDP-DP-549, Nov. 2017, available at: https://publications.iadb.org/publications/english/document/The-Impact-of-Digital-Innovation-and-Blockchain-on-the-Music-Industry.pdf (accessed on 05 February 2021).

[30] For some examples: see on Sotheby's website https://www.sothebys.com/en/buy/auction/2021/this-changed-everything-source-code-for-www-x-tim-berners-lee-an-nft (accessed on 28 June 2021) or the Times https://time.com/5947720/nft-art/.

[31] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf (accessed on 17 February 2021).

[32] http://blockchainlab.lu/projects/.

[33] See for example: https://www.ledgerinsights.com/axa-blockchain-flight-delay-compensation/ (accessed on 17 February 2021).

on the market value attached to such use cases and therefore on the economics behind smart contracts and their deployment.

In this respect, one of the most obvious benefits of smart contracts is the reduction of non-execution risks (zero third party trust process) thanks to the automation of the execution process. However, as of today, only obligations that can be fully automated (reliance on digital assets or automation of delivery) can be supported by smart contracts. By contrast, when a contractual obligation relates – for example – to the delivery of physical assets, this would first require a full automation of the supply and delivery chain.

As discussed above, other economic benefits of smart contracts and the underlying blockchain or DLT in the case of legally binding agreements are to:

- ensure the timely settlement of any (financial) transactions, by embedding adequate information to this effect in the code underlying the smart contract and implementing adequate data feed from third party agreed sources, when required (the so-called oracles[34]);
- simplify reconciliation process, with respect to (financial) transactions by having a shared and trusted ledger containing the necessary data flows; and, as a result,
- reduce litigation risks.

Underlying technological costs should not be underestimated, and a proper costs/benefits analysis should be performed. A similar approach should be adopted with respect to risks associated with smart contracts and DLT. For instance, depending on the architecture supporting the DLT, risks will differ in public or private blockchains.

Economic benefits of smart contracts are especially relevant for financial transactions where the payment or delivery of financial assets is critical and time efficiency is essential. Traditionally, transactions in which errors or delays can have a huge financial impact for the parties – such as derivative agreements or other financial transactions where payment versus delivery (or delivery versus delivery) is a critical feature – often require the involvement of a trusted third party to ensure a timely and secure completion and settlement of the relevant transaction. In such a context, smart contracts offer considerable efficiency gains by reducing or even completely removing the need for such third party intermediaries.

[34] Please refer to Appendix 2 - the Glossary - for a definition.

2. The main legal challenges associated to Smart Contracts

Luxembourg laws and especially the Luxembourg Civil Code contain detailed provisions on contracts and contracting. These provisions govern notably (i) contracts' formation and the conditions contracts must fulfil to be valid and enforceable, (ii) their content and effects (including performance and means to maintain a balance of powers between the parties), and (iii) legally acceptable enforcement measures with respect to contracts' performance. The general legal principles laid down in the Luxembourg Civil Code were often successfully applied to new human activities by lawyers and courts. As a result, assessing the challenges that Luxembourg (contract) law may present with respect to the adoption of smart contracts appears almost as a necessity. However, we argue herein that amendments to the legal framework should only be proposed as a last resort where a clear legal need is identified.

This chapter focuses on the main challenges identified by the SC Working Group during the Survey. Most of these challenges were already raised to a certain extent by various legal authors, but not specifically from a Luxembourg legal perspective.

In a first section, smart contracts will be analysed through the lens of contract law. The goal is to highlight points to pay attention to when structuring a smart contract, whether as the only agreement existing between the parties or as the means of execution of a separate (legal) agreement.

The second section will briefly introduce the challenges that might arise when looking to adequately protect the smart contract *per se*.

The last section will focus on the need to assess data protection principles at an early stage of the design of a smart contract, in a privacy by design mode.

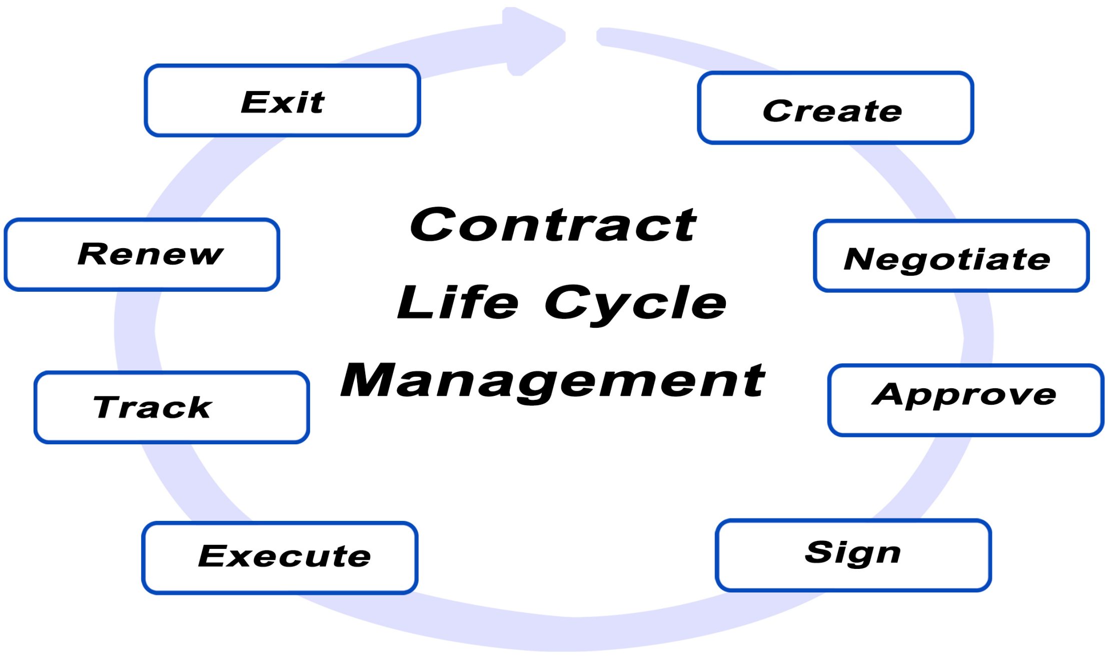
The SC Working Group has however decided not to address herein issues related to the liability of the players involved in the design and functioning of a smart contract[35] and to applicable law and competent jurisdictions. These issues are often already addressed with respect to the DLT and are not necessarily specific to smart contracts.

[35] For interesting analysis on Blockchain/DLT and liability see: Dirk Zetzsche, Ross P. Buckley and Douglas W. Arner, "The distributed liability of distributed ledgers: legal risks of Blockchain", University of Luxembourg law working paper n. 007/2017, available on SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214; Luigi Buonanno, "Civil liability in the era of new technology: the influence of Blockchain", Bocconi legal studies research paper n. 3454532, sept. 2019, available on SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3454532.

2.1 Smart contract: a means to conclude or to execute a legally binding agreement?

There are two main phases in the lifecycle of an agreement:

- the formation phase, where parties discuss and agree on the terms of the contemplated agreement, which is documented if deemed appropriate or legally required (a prerequisite being the willingness of these parties to enter into a contractual relationship), and
- the execution phase, where parties perform their respective obligations as agreed in the agreement, i.e. the contract produces the agreed legal effects.



Smart contracts could be used during one or both phases described above. Such use will however depend firstly on the will of the parties and then on whether compliance with the provisions of the Luxembourg Civil Code and/or other relevant legislation can be ensured when deploying the smart contract.

This section aims to outline the result of the SC Working Group's discussions in this respect, and notably to clarify how the existing Luxembourg legal framework could apply to smart contracts and what are the points that should be considered to ensure that smart contracts would have the legal effects contemplated by their designers and users in the context of the Luxembourg contract law.

2.1.1. Smart contract, already a means to conclude an agreement?

Agreeing on the terms of a contract can take various forms: (i) verbal – for example when buying our bread –, (ii) fully digitised – i.e. purchase through online applications on our computer or smartphone –, (iii) in writing or (iv) in writing while also respecting a legally prescribed form, e.g. a notarial deed when buying a house, etc. Nowadays, contracts may be deemed in writing despite the absence of traditional paper support. The current COVID 19 pandemic has even accelerated the digitalisation movement with the use of tools such as DocuSign.

According to 75% of the respondents, smart contracts should be deemed to be in writing. This leads to the conclusion that the use of programmable language to write smart contracts and the use of DLT-based platforms to host them should arguably not preclude a smart contract from qualifying as a written contract. In their comments, respondents to the Survey emphasise on the need to ensure that conditions for legal validity of contracts are first and foremost complied with.

No Luxembourg legal provision expressly prevents a smart contract to be fully equivalent to a legally binding agreement. However, as for which smart contract can legally qualify as a contract remains to be determined in accordance with Luxembourg Civil Code. The Code provides a definition of what a contract is in its Article 1101, whereas its Article 1108 lists the "Four requirements [which] are essential for the validity of an agreement [i.e.]:

- The consent of the party who obligates herself;
- That party's capacity to contract;
- A definite object that forms the subject matter of the engagement;
- A licit cause for the obligation."

For a smart contract to be qualified as a (legal) contract by judges or lawyers, the above conditions would need to be fulfilled. For this purpose, the SC Working Group considers that the following points are critical and should therefore be addressed in more details:

- the identification of the contractual parties must be possible in order to allow the verification of the consent and the capacity conditions (including, notably, age, suitable authorisation if such authorisation is legally required, etc.); and
- the terms of the smart contract must be understandable and verifiable in order to establish the object on which the parties agreed and the cause of the contract.

2.1.1.1. Agreeing to contract or the need to identify the parties to a (smart) contract

By definition, a legally binding agreement requires two or more parties to it. This may not always be the case for smart contracts. When an issue arises regarding the existence, the validity or the execution of contractual obligations, a first step should be to determine who the contractual parties are. This appears to be a prerequisite to establish whether or not parties have consented to the agreement as well as to confirm their capacity and authority to enter into the contractual relationship.

Depending on the medium (*instrumentum*) through which the agreement is concluded, identifying parties to agreements might differ. When an agreement takes a written form (including a digital one) – either as a result of applicable legal requirements or as a result of the choice of the parties –, one shall refer to the signatories and their signature. In this case, signatures must meet certain requirements detailed in Luxembourg Civil Code[36].

Smart contracts involve a signature mechanism and would generally embed no further identification details relating to the signatories. Identifying the signatures may therefore be the only way to identify the signatories.

Signatures used in smart contracts are often referred to as "digital signatures" and relate to the cryptographic mechanisms used to implement electronic signatures. As of today, there is no definition in the European or Luxembourg legislation of a digital signature. However, according to International Standard ISO 22739:2020, digital signature could be defined as "data which, when appended to a digital object, enables the user of the digital object to authenticate its origin and integrity".

These digital signatures are in principle generated and verified through standardised frameworks such as the Digital Signature Algorithm (DSA)[37]. There are typically three algorithms involved with the digital signature process:

1. Key generation – This algorithm provides a private key along with its corresponding public key;
2. Signing – This algorithm produces a signature upon receiving a private key and the message that is being signed;
3. Verification – This algorithm checks for the authenticity of the message by verifying it along with the signature and public key.

In summary, digitally signing smart contracts requires that the signature generated by both the fixed message and the private key can be authenticated by its accompanied public key. Using these cryptographic algorithms ensures that the user's signature cannot be replicated without having access to his/her private key. This digital signature does not however automatically qualify as an electronic

[36] Luxembourg Civil Code, Article 1322 and subs.

[37] See for e.g. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

signature within the meaning of eIDAS Regulation and thus does not have the legal value attached thereto when it relates to the identification of the parties.

According to 50% of the respondents to the Survey, the signature of a smart contract should not raise specific concerns. For those who raised concerns, the main issue related to compliance with the eIDAS Regulation requirements and to security.

Under current laws and regulations[38], only a qualified electronic signature as defined below would produce a legal effect equivalent to the legal effect attached to a wet-ink signature, and will be deemed to offer a sufficient degree of confidence in the electronic identification means[39].

The "electronic signature" itself is defined as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"[40]. Different types of electronic signature are recognised in various jurisdictions. The EU has issued prescriptive and precise criteria for a qualified electronic signature to be deemed equivalent to a wet ink-signature, including the involvement of a trusted third party and a country specific supervisory body. An example of qualified electronic signatures that Luxembourg residents use regularly is the certificate issued by LuxTrust which is subject to the supervision of the ILNAS.

A key difference between the digital signature and the electronic signature is thus the absence, in the case of the digital signature, of a trusted third party service provider to ensure a high level of security. Ensuring such security ultimately has implications on the legal certainty of the digital signature and the identity of the underlying signatories. This difference can be explained by the libertarian philosophy behind the initial use of the DLT (i.e. the Bitcoin). Broadening the use of smart contracts in our daily lives may require a partial waiver to the anonymity or pseudonymity offered by the digital signature: A party to a contract often

[38] See eIDAS Regulation, especially Article 25 thereof.

[39] eIDAS Regulation, whereas (16).

[40] eIDAS Regulation, Article 3 (10); see also the e-signature FAQ, published by the European Commission (CEF Digital) (accessed on 30/11/2020) for criteria of distinction retained at European level. In most countries, electronic signatures must meet the following criteria: (i) the signatory can be uniquely identified and linked to the signature; (ii) the signatory must have sole control of the private key that was used to create the electronic signature; (iii) the signature must be capable of identifying if its accompanying data has been tampered with after the message was signed; (iii) in the event that the accompanying data has been changed, the signature must be invalidated.

wishes to know with whom he/she contracts. The identification of the parties is also a legal requirement for contracts, including notably *intuitu personae* agreements.

As of today, various discussions are taking place at European and international levels[41] to determine criteria that could be agreed for the recognition of private keys used in the DLT environment, initially in the context of e-identity. The impact of any agreement reached at supranational level and how such agreement will be implemented in Luxembourg should therefore be monitored.

Determining and understanding the legal qualification of the private key required for smart contracting is also important to determine the legal value of a smart contract as evidence in case of dispute relating to the conclusion or performance of the smart contract. Consequently, this issue should be addressed upfront, either from a technical viewpoint or from a contractual perspective.

From a technical point of view, one needs to ensure that the signature process of the smart contract fulfils the legal criteria of electronic signature to the extent technically possible. From a contractual viewpoint, one needs to clarify the legal value to be given to smart contracts and their signature process, taking into account the principle of contractual freedom.

Adequate identification of the user of an electronic signature may also be required to ensure compliance with the requirements of the Financial Action Task Force ("FATF") as well as the EU and Luxembourg legislations on the fight against money laundering and terrorist financing. Considering existing publications on the subject, we have not specifically addressed it herein[42].

Once the parties to a smart contract are identified, it is possible to determine if they are capable of entering into the terms of the agreement using a smart contract to this effect. This identification also helps to assess the validity of their consent if such validity was to be challenged *ex post*.

This assessment shall be made in accordance with applicable laws. For this purpose, embedding verifications relating to the capacity or the consent of the parties in the underlying code of a smart contract is crucial, although it may prove to be challenging for the time being, at least from a legal point of view. Except with the support of adequate and reliable external databases, the capacity of a person is in principle determined by his/her national law, while the validity of a

[41] https://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-digital-id-nov-2019.html.

[42] FATF Report on Virtual Currencies : Key Definitions and Potential AML/CFT Risks, https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html, and other FATF related publications available on https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate), accessed on 2 March 2021.

consent often requires detailed factual assessment and, therefore, data likely to be only accessible off chain.

2.1.1.2. Agreeing on the content of a smart contract or the importance of assurance mechanisms

Parties to an agreement, which involves the implementation of a smart contract to support its execution, may seek assurance that the codes or algorithms underlying the smart contract adequately capture the terms of their agreement. This is notably the case where the smart contract relates to the issuance or transfer of digital assets or more generally, leads to the automated performance of contractual obligations.

As briefly mentioned previously, parties would therefore seek assurance from a third party expert to audit the code prior to its deployment in practice. The audit process aims, on one hand, to verify and certify that the code underlying the smart contract reflects the terms of the legal agreement and, on the other hand, to prevent users from exploiting any errors or inconsistencies in the code. Such auditing shall take place before the implementation of the code in the DLT, and is referred to as an *ex ante* audit.

Given that coding accurately certain terms of a contract may be difficult from a technological perspective and since errors in the code itself or in the outcome it produces can occur, parties to an agreement seeking to implement a smart contract should carefully consider addressing these risks (including issues related to performance that the auditing process may not have uncovered) in their legally binding agreement by, for instance, agreeing contractually that one of the parties will bear the risks related to any misuse of the code.

Provided that the same code (underlying a smart contract) is used in the same context, it should normally not be required to have an audit or assurance review performed by an independent third party each time a new smart contract using the same code and functionalities is implemented by the same or by different parties. However, it would be advisable to carefully check any changes to the code or other (external) inputs triggering the need of a new audit or assurance report, considering potential security vulnerabilities such changes or input can create in the code or the smart contract itself or the new functionalities they may aim to implement.

As of today, there is no standard regarding smart contracts or blockchain/DLT audit or assurance performance (and related reports) that is comparable to International Standards on Assurance or Auditing Engagements[43]. For instance,

[43] For further details, please refer to the website of the International Auditing and Assurance Standards Board: https://www.iaasb.org/standards-pronouncements (last accessed on 31 March 2021).

the costs of such audit/assurance vary depending on the complexity of the code and contemplated functions.

Having industry standards applied to audit/assurance performance would foster trust in such processes. Various organisations have initiated standardisation work in this context, in particular the ISO, with respect to technical standards[44]. Audit standards might possibly be part of this work.

In addition to the audit or assurance process, it is highly recommended when setting up a new smart contract or amending (one of) its features to involve an independent third party (e.g. for writing or testing the code), as the involvement of such independent expert may also be required in case of litigation relating to the proper execution of the smart contract. In particular, this may be necessary when there is a need to evidence that the algorithms and code used are adequate and that they correctly translate the intention of the parties, which is usually based on the underlying traditional legal contract. The need to do so may for example derive from *ex post* audit or forensic examination. In such case, an adequate level of expertise of the independent third party will be required.

More generally, fostering the use of DLT might also come from the standardisation of the audit process and the blockchain or DLT technical standards. Such standardisation would improve the understanding, interoperability and trust in relation to smart contracts, and will facilitate the audit process, in the same way as standardisation of accounting and audit standards helped improve trust in the financial statements of companies (and therefore boosted the financing of their corporate activities). It would also help ameliorate the understanding of the audit or assurance process and create minimum market standards that could serve as reference for the various stakeholders, including lawyers and judges. Finally, in case of litigation, judges, arbitrators and other involved parties will be able to properly understand how the intention of the parties was reflected in the smart contract brought to their attention.

To conclude, where parties remain free as to the choice of the form of their agreement, the key limit to the use of smart contracts may result from their digital form and computerised language. These features currently restrict their use to transactions in digital assets, even though such transactions must be simple enough for all their terms to be automated (i.e. there is no need to factor unforeseen events or a possible recourse to default provisions of Luxembourg law for any point not provided for by the smart contract). As a result, smart contracts tend nowadays to be mainly used to enable an automated execution of some part

[44] https://www.iso.org/committee/6266604.html (last accessed on 16/06/2020).

of the contractual obligations of the parties rather than a (more traditional) legally binding agreement.

2.1.2. Smart contracts, mainly means to execute contractual obligations

The performance of a contract always involves risks, such as the risk of default by a party or the risk of partial or erroneous performance, or a change in the conditions governing its execution, namely an unforeseen event rendering the execution onerous or even impossible. Depending on the impact that such an event would have on the contract, a party thereto may suffer damages or additional costs. The duration of the contract may lower or increase these risks. In order to mitigate such risks, the parties often look for suitable mechanisms or contractual provisions adjusted to the duration of the contract, the obligations to be performed, etc.

Smart contracts can be seen as one of these useful mechanisms to execute contractual obligations, whenever the agreed obligations can be automated. The support of oracles may further be envisaged if needed. Smart contracts are in particular suitable for long term contracts where the obligations agreed between the parties are recurring and can be standardised.

However, smart contracts must be more detailed and formalised than (ordinary) contractual terms expressed in a natural language: The code cannot be ambiguous. Considering its underlying mathematical language, code should normally be clearer and less prone to errors than natural language. Errors may nevertheless be still contained in the code as the code is a translation of the agreed contractual terms, as understood by the coder of the smart contract.

Translation into computerised lines of all the usual terms of a contract does not appear to be operationally possible as of today. Otherwise, it would mean being able to capture and translate into binary language and lines of code not only a considerable number of usual contractual terms but also real-life events that may be associated thereto.

Clauses of hardship or clauses of "force majeure" are typically examples of contractual provisions that are difficult to automate and, therefore, to embed in a smart contract[45]. This would in particular be the case if the parties wish to opt for a definition of "force majeure" broader than the one that is currently recognised by Luxembourg case law or to tailor it to the specificities of their activities and markets, such as cloud service providers subject to enhanced security duties. Such

[45] See for a detailed analysis: Eric Tjong Tjin Tai, "Force majeure and excuses in smart contracts", Tilburg private law working paper series n. 10/2018, available on SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3183637.

clauses aim to address unforeseen or adverse events that may occur during the lifecycle of an agreement and that affect its terms and execution. As of today, automating these provisions would therefore require using external reliable sources for data that are likely to evolve overtime, such as databases with respect to events qualifying as unforeseen, events under relevant laws and regulations and related case law (such as war, terrorism, riots, government actions, pandemics, natural disasters). These databases would need to be carefully designed and built and may require human intervention for analysis and interpretation in order to ensure that the system relies on current and up-to-date data.

Most of the respondents to the Survey considered nevertheless that smart contracts do not necessarily need to be complemented by contractual provisions handled out of the chain, as all provisions could probably be inserted in the smart contract itself. One respondent even asked: "Why are you doubting this?".

Practical use cases however show that smart contracts are first and foremost used in the contractual space to automate the performance of specific contractual obligations, with the aim, on one side, to reduce the risk of poor performance or non-performance and associated costs (financial costs, litigation, interaction with connected financial transactions, etc.) and, on the other side, to complement traditional contracts initially agreed between the parties. A smart contract could therefore be seen as an automation of the execution of certain obligations of the parties. It could also serve to automate the termination of the contract upon the occurrence of contractually agreed events.

The existence of a traditional legal agreement alongside a smart contract will however require the implementation of suitable legal and technical solutions to properly link both "contracts". The hash function may be useful for this purpose as discussed in the following section.

2.1.3. Building a bridge between smart contracts and their related agreements

Smart contracts are currently part of, or the result of, a pre-existing legally binding agreement which is often considered as a framework agreement. It may therefore be necessary to build an adequate link between a smart contract and the relevant framework agreement to which it relates, not only as part of the contractual provisions, but also within the scripts used to design and build the smart contract.

A current technical solution consists in embedding in the smart contract, the legal clauses of the framework agreement, or even the contract itself, as a hash. This enables the possibility in the future to know – thanks to the properties of the hash and the immutability of the blockchain – whether or not the clauses or the contract have/has been amended or even falsified. However, to do so, the original agreement must be kept outside the blockchain in order to be able to retrieve it and access its content: The use of the hash here makes it impossible to retrieve a readable version thereof in the blockchain itself. In this case, the hash should be seen as a proof of authenticity of a document stored on the blockchain and not as the storage of the document itself.

Given the immutability nature of the blockchain – i.e. it is not possible to modify or delete information stored on the blockchain –, once a smart contract is deployed on the blockchain, it will no longer be possible to modify any of its elements. Therefore, if there is a need to amend, modify and/or update the smart contract to reflect new terms agreed by the parties, new legal or regulatory requirements, or even to correct it, the simplest technical way to do so will be to design and build an *ex ante* self-destruction function into the initial smart contract[46]. For this purpose, *ad hoc* code lines must be contained in the smart contract. Such function will render the initial smart contract permanently inaccessible and it will then deploy a new smart contract with the desired modifications.

In addition, if more than one version of the smart contract should coexist, then the new smart contract will have to be associated with each related version, in a similar manner as amendments to traditional legal agreements[47].

2.2 Smart contracts and IP/IT rights

Protecting IP rights has always been critical for organisations due to the economic value attached to technical developments, content creation, etc. Having a closer

[46] On various issues and an interesting discussion in this regard see e.g. Eric Tjong Tjin Tai, "Force Majeure and Excuses in Smart Contracts"(May 4, 2018), Tilburg Private Law Working Paper Series No. 10/2018, accepted version published in European Review of Private Law 2018/6, p. 787-904., available at SSRN: https://ssrn.com/abstract=3183637.

[47] Olivier Poelmans, *Droits des obligations au Luxembourg*, Les Dossiers du Journal des tribunaux Luxembourg, Edition Larcier, Partie 2, Titre 1, Chapitre 4, Section 4.

look of the history behind some key inventions can be very instructive in this respect. *Ad hoc* national and international legislations and treaties were adopted over time[48] to allow organisations or more generally inventors to benefit from IP rights (both morally and mainly financially). These legislations and treaties are reviewed on a regular basis to ensure a better protection of new inventions, especially in the current digital environment.

Organisations which develop smart contracts often address IP rights during the development phase. They might thus consider using enhanced technical measures to digitally manage and protect their IP rights[49] or seek adequate legal protection thereof, or both. A quick search with the terms "source code" and "smart contract" in the WIPO patent register or in the one maintained by the European Patent Office may give indications of current trends in this area[50]. It also evidences the willingness of organisations developing smart contracts to protect them through various means, even when smart contracts rely on open source software.

Smart contracts would normally qualify as software considering the definition of software provided by the WIPO in its Model provisions on the protection of computer software of 1978[51] and as computer program following the definition provided in the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (the "Computer Programs Directive")[52]. They should therefore be regarded as a literary work in the sense of the Berne Convention for the protection of literary and artistic works and thus be subject to protection by copyright, without the need of a prior registration.

As all other literary works, software and therefore smart contracts should be original in order to benefit from copyright protection. In the EU, a smart contract shall be the "author's own intellectual creation" in order to be considered as original and "No other criteria shall be applied to determine its eligibility for

[48] https://ec.europa.eu/info/business-economy-euro/doing-business-eu/intellectual-property-rights_en.

[49] Finck, M., Moscon, V. Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC* 50, 77–108 (2019). https://doi.org/10.1007/s40319-018-00776-8.

[50] https://patentscope.wipo.int/search/en/result.jsf?_vid=P21-KKQYGO-94665.

[51] Software comprises "*a set of instructions capable, when incorporated in a machine-readable medium, of causing a machine having information-processing capabilities to indicate, perform or achieve a particular function, task or result*".(WIPO, Model provisions on the protection of computer software, Geneva, 1978).

[52] *For the purpose of this Directive, the term 'computer program' shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.* (Whereas (7) of the Computer Programs Directive), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0024 (accessed on 24 March 2021).

protection"[53]. No valuation of the quality or the aesthetic value of the program will be needed in order to determine if a smart contract can be protected by copyright.

However, copyright alone is not a sufficient protection: It does not apply to ideas or principles which underlie interfaces (Article 1.2 of the Computer Programs Directive). As a result, in Europe and therefore in Luxembourg, it will mainly protect preparatory design material, source and object code, and structure and architecture of smart contracts. Copyright can however not protect the programming language, the algorithms or the functionalities of these smart contracts. In addition, the rights of smart contracts' authors relating to the very exploitation of these smart contracts would be limited by:

- their obligation to allow the decompilation and reproduction for interoperability grounds in specific circumstances and subject to specific safeguards[54];
- the adaptation or correction of the smart contracts required for its use in accordance with its intended purpose[55]; and
- the permission of a lawful user of a smart contract to create a back-up copy.

Complementary means to protect smart contracts should therefore be considered and normally used in a cumulative manner with the former, especially when taking into consideration the potential need for smart contracts developers to gain worldwide protection (depending on the selected DLT platform). These other means are usually:

- the protection of any trademark associated to a smart contract: the protection being then limited to the specific name attributed to the smart contract or to its underlying language, with the aim to develop and protect the reputation of the smart contracts;
- protection via patents, with a scope that may vary depending on the countries: Patents are normally granted for processes and products, and smart contracts are likely to be viewed as mathematical methods like software and not considered to be subject matter for patent protection. The trend seems however to accept patent registration associated to smart contracts, but in the patent application, the registrant would not claim the smart contracts as such[56];
- a protection of the design, only with respect to the graphical interfaces, graphics or icons; or

[53] Article 1(3) of the Computer Programs Directive.

[54] Article 6, Directive 2009/24/EC of the Computer Programs Directive.

[55] Article 5(1), Directive 2009/24/EC of the Computer Programs Directive.

[56] See WIPO patents registry for examples of smart contracts related patents' registrations.

- the protection of trade secrets[57] which underline smart contracts, if and to the extent the conditions provided in various legislations, including those transposing the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure[58], are complied with. Such protection shall be especially relevant to protect the algorithms, to the extent they qualify as trade secrets (i.e. a secret, having business value, whether actual or potential, specifically for being secret, and being (or having been) subject to suitable measures to keep them secret)[59].

It is therefore critical that the deployment of a smart contract on a DLT platform does not lead to the disclosure of the algorithm or other information to be protected mainly by trade secrets legislation. It is also essential to, at least, insert *ad hoc* confidentiality clauses in the related agreements or in the terms governing the DLT platform. In practice however, the latter case may be easier to do in the context of a private or permissioned blockchain rather than in the context of a permissionless or public blockchain.

Protecting the investments made to develop smart contracts may also require protecting not only the IP rights – that may be directly attached to smart contracts –, but also those which may be attached to the supporting DLT platform and related databases. Considering the scope of this White Paper, these points have not been specifically discussed and no further analysis is provided herein in this regard.

2.3 Towards Compliance with EU Data Protection Legislation

How smart contracts and DLT supporting platforms can comply with the (EU) General Data Protection Regulation 2016/679[60] is probably one of the main challenges to be decisively resolved in order to promote a broader adoption of these innovations in a permissionless and borderless environment. Studies have even been commissioned at the level of the EU to determine how GDPR requirements could apply to blockchains, despite obvious tensions. This is notably

[57] Protecting trade secrets: how organizations can meet the challenge of taking "reasonable steps".

[58] The full text of the Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (or the "Trade Secret Directive") is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

[59] *Cf.* also the definition of 'trade secret' provided by Article 2(1) of the Trade Secret Directive.

[60] The full text of the GDPR is available at https://eur-lex.europa.eu/eli/reg/2016/679/oj.

the case of the study on the Blockchain and the General Data Protection Regulation (the "Study")[61] published in July 2019 by the European Parliament.

In principle, any direct or indirect processing of personal data via a smart contract hosted on a DLT platform may fall within the material and territorial scope of the GDPR. This regulation has indeed a very broad territorial and material scopes of application and provides broad definitions of personal data[62] and processing[63]. The vast majority of the respondents to the Survey acknowledged this. They also highlighted associated challenges. This section aims to address some of those challenges. Publication of guidelines by the European Data Protection Board (the "EDPB") in the near future[64] should help clarify this matter.

2.3.1. Areas of frictions between DLT and GDPR

At first sight, the GDPR and distributed ledgers seem entirely incompatible. The regulation seeks to give data subjects control over their own personal data (including a right to request their erasure or to object to certain data processing), while arguably one of the most attractive characteristics of distributed ledgers relates to their immutability. Further, the drafters of the GDPR seemed to assume that data subjects' personal information would be controlled and processed by easily identifiable actors (primarily the data controllers), to whom data subjects would turn to in order to enforce their rights. Finally, while they addressed the delegation of processing to data processors and the existence of joint-controllers, the drafters of GDPR did not consider the possibility that data storage, as well as data processing, may be performed in a decentralised context by multiple players whose functions may be interchangeable, a feature which however lies at the core of DLT. Allocation of roles and responsibilities across various players and implementation by those players of adequate safeguards for any transfer of the personal data outside the EU may therefore prove challenging.

[61] Please consult full version of the Study at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[62] See Article 4(1) of the GDPR.

[63] See Article 4(2) of the GDPR.

[64] EDPB Work Programme 2021/2022, Pillar III - A fundamental rights approach to new technologies, https://edpb.europa.eu/our-work-tools/our-documents/work-programme/edpb-work-programme-20212022_en (accessed on 18 March 2021)

However, stating that DLT can never be GDPR compliant runs the risk of oversimplification. Having in mind the core principle of privacy by default and by design laid down in the GDPR, entrepreneurs and organisations of all sizes seeking to rely on DLT can take a number of steps at an early stage of their projects to achieve compliance with the GDPR. In this respect, they should factor in the state of the technology, the intended core features of their products and the type of DLT platforms used (permissionless or not, etc.).

This being said, legal uncertainty exists as to how certain data protection principles would apply in a decentralised and distributed context, especially in the absence as of the date of this paper of guidance from the EDPB or from the Luxembourg *Commission Nationale pour La Protection des Données* (the "CNPD"), on the one hand, and of case law relating to DLT platforms or blockchain, on the other hand.

An overview of certain data protection issues that are critical and cannot be overlooked when using smart contracts and DLT as well as guidance that may assist organisations in achieving compliance with GDPR are provided in the following sub-sections.

2.3.2.Determining respective roles and responsibilities

The GDPR allocates different responsibilities to the various persons likely to be involved in the processing of personal data. These responsibilities depend on their respective roles. Determining these roles is fact-based, on a case-by-case basis for each and every processing. For example, the same person may act as controller when he/she processes personal data to perform know-your-customers checks and as processor when he/she transfers virtual assets according to instructions from a client.

While no EDPB or CNPD guidance is currently available to perform such analysis for smart contracts actors, the approach generally taken with respect to software and cloud hosting could serve as a good starting point. We therefore think that the following specific points should be considered and documented:

At the level of the applications hosted on the DLT platforms such as smart contracts:

- Developers: Are they responsible for determining the purpose of the processing linked to the smart contracts and/or part or all of the means used for this data processing? Do they even need to process personal data at this stage?

In some instances, developers can only create the algorithmic program first off chain, use anonymised data for testing and then publish the program on the DLT (i.e. there is no personal data processing in this scenario).

- Persons hiring the developers: Are they providing the expected specifications of the applications and processing details? What is their authority to determine the personal data processed or the outcome of the smart contracts? Such persons are more likely to be seen as the data controller(s), rather than the developers;

At the level of the DLT platforms, depending on the features of the platforms (private vs public, etc.) and the processing under review:

- Nodes: What would be their involvement in the validation process and therefore in the architecture and governing rules applicable to the DLT platform? They could either qualify as processor or as joint-controllers regarding the processing of any personal data hosted on the DLT platform and the validation of blocks and their maintenance of a duplicate register;
- Miner: The description of their functions in the DLT platforms' governing rules should be carefully considered to determine their legal responsibilities and related status under GDPR. While miners could have significant control over the means of the processing, they should have only limited control over the processing's purpose. However, it may not be possible to always exclude miners' qualification as processors and the legal consequences associated thereto;
- User: Here again a fact-based analysis will have to be performed, taking into account the architecture of the DLT platform, the DLT governing rules and operating processes, etc. to determine when a user is acting as (joint) controller or as processor, as it seems unlikely that a user will be out of scope of the GDPR.

Once the respective roles and associated responsibilities of the various stakeholders are clarified, adequate contractual provisions must be adopted and relevant disclosure to individuals whose personal data is recorded and shared, must be carried out.

Data processing by a processor must be governed by a contract between the processor and the controller, the terms of which are specifically detailed in Article

28 of the GDPR. Joint controllership also requires *ad hoc* contractual provisions to be agreed between the parties to determine their respective responsibilities for compliance with the GDPR, especially with the exercise by data subjects of their rights (Article 26 of the GDPR). This again may be challenging, even more so when the smart contracts are published on a public blockchain where participants may be located worldwide and may be free to join. Including adequate information in the documentation governing the supporting blockchain (e.g. responsibilities of the various players, consequences associated thereto, processes in place to facilitate the exercise of data subjects' rights, etc. and clarifying the legal value of such documents) might be one option to be carefully considered.

2.3.3.Compliance with overarching principles relating to personal data processing

Data controllers are responsible for compliance with several overarching principles relating to personal data processing, including lawfulness, accountability and transparency (Article 5 of the GDPR) and more generally the principle of privacy by default and by design. In a distributed environment, ensuring strict compliance may prove difficult for the multiple players involved and primarily for those likely to qualify as controllers. One must therefore have a clear picture of these difficulties before developing a smart (legal) contract.

A first step may be carrying out an assessment of the suitability of this technological solution for the processing of personal data associated thereto. As shown by the Study as well as the paper[65] issued by the French data protection authority, the Commission Nationale Informatique & Libertés ("CNIL"), the features and the architecture of the underlying DLT platforms have a significant impact on the analysis.

Another way to reduce compliance challenges may be to minimise personal data use or to use all suitable technical means available to render personal data on the chain as anonymous as possible. This might help to comply with the requirement to implement adequate technical and organisational measures (Article 32 of the GDPR).

From a security standpoint, the authors of the Study also suggest to use and implement all possible measures for the creation of hard barriers between personal data which must unavoidably be stored on chain and any off-chain data storage.

For the purposes of minimising personal data storage on DLT platforms, initiators of smart contract projects should carefully consider the format they will use to link

[65] Blockchain - Premiers éléments d'analayse de la CNIL, September 2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, last accessed on 24 March 2021.

personal data to data stored on the platform upon deployment. Technical solutions to prevent direct storage of personal data on the DLT platform exist. For example, personal data could be stored off-chain whenever possible or personal data that needs to be on-chain could be hashed in order to make it anonymous. In the latter case, the hash would then be stored as input[66] for the smart contract and used as a proof of authenticity, instead of using the initial personal data that was anonymised.[67]

The use of state of the art encryption, hash functions with the strongest privacy guarantees and other pseudonymisation techniques is also recommended to achieve and maintain the highest degree of security overtime.

The CNIL also recommends similar technical measures "to enable stakeholders to come closer to the GDPR's compliance requirements, in particular by blocking access to data depending on the format chosen (e.g., commitment, fingerprint generated by a hash function with a key, encryption, etc.)"[68] .

It is not an option for most of the smart contracts projects to be fully out of the scope of the GDPR, as this would mean no processing of personal data by any of the actors involved (including no data relating to digital keys). In this context, ILNAS expressed the view that privacy offered via a DLT platform is in principle limited to pseudonymisation of the transactional data and the keys related data.[69]

2.3.4.Allowing data subjects to exercise their rights of rectification and erasure

The GDPR requires that personal data can be modified or erased at any time at the request of any data subject or that data processing can be stopped, considering the rights granted to data subjects. DLT renders such modifications or erasure purposefully onerous in order to ensure data integrity. Thus, enabling data subjects to exercise their rights is not straightforward in a DLT context.

As of today, neither the EDPB, nor the CNPD have issued specific guidance in this respect yet. By contrast, the French and British data protection authorities have issued guidance on the acceptable means to achieve the modification or erasure

[66] For more details regarding the concept of "input", please refer to: https://cointelegraph.com/news/what-are-inputs-and-outputs (last accessed on 10 June 2020).

[67] More details regarding the use of the hash function to ensure compliance with GDPR can be found in the Study as well as in a specific essay jointly published by the Agencia Española de Protección de Datos and the European Data Protection Supervisor in October 2019. This essay can be found at https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_fr (last accessed on 18 February 2021).

[68] www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (last accessed on 10 March 2021).

[69] ILNAS, Blockchain And Distributed Ledgers, Technology, Economic Impact And Technical Standardization, July 2018.

of personal data when a straightforward deletion or modification appears technically impossible[70]. This guidance could help in order to work on acceptable technical solutions. Here again the controller(s) or initiator(s) of the project should perform a case-by-case analysis the results of which should be adequately recorded and stored.

For example, the UK Information Commissioner's Office ("ICO") suggested, as an alternative to amendment or deletion of personal data, that this data may instead be "put beyond use": even if not actually deleted, provided that the data controller holding such information meets certain conditions (no future use of the personal data, no granting of data access to third parties, implementation of adequate security measures, and deletion of the personal data once it becomes feasible).

The French CNIL even recommends some technical cryptographic measures. As discussed above, the cryptographic hash function is seen as a useful tool to allow compliance with the right to be forgotten and related data deletion right, despite the immutability of the blockchain on which the data may be stored. Here, emphasis is put on the outcome of the hash function – future irreversible lock of the access to, and the processing of, the personal data that may be embedded in a smart contract or available on the DLT platform –. However, proper equivalency to the GDPR requirements should be assessed.

When working on an acceptable technical solution to address the GDPR erasure right, one may need to keep in mind that:

- The right for deletion is not an absolute right (balance between the various fundamental rights in presence is to be performed) and applies only in certain limited circumstances;
- No definition of the term "erasure" is provided by the GDPR and the EDPB has provided no guidance on its interpretation so far;
- For personal data made public, controllers may take into account available technology and the implementation costs of any assess steps to be taken;
- Deletion in a blockchain environment cannot be done in the same manner as in a paper-based environment or in a traditional digital environment;
- GDPR should be a technologically neutral legal framework. It does not aim to hinder technological developments which are deemed generally useful, especially in the light of the European Digital

[70] France: https://www.cnil.fr/fr/limiter-la-conservation-des-donnees (final archiving authorised in limited circumstances), and https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651957, United Kingdom: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/).

Strategy and the implementation of the European Blockchain Observatory and Forum. As a result, tensions noticed regarding blockchain technology and GDPR should be solved while general principles of law and fundamental rights – such as the right to conduct a business and the right to privacy – should be reconciled;

- GDPR aims at favouring tools that enable individuals to retain control over their own personal data; and
- The outcome of the hash function would be to render personal data inaccessible by anyone and in an irreversible manner: When properly implemented, the hash function should therefore irreversibly prevent the identification of the individual whose data is embedded in the smart contract by any person other than himself/herself.

In any case, a cautious approach when coding a smart contract seems to include functionalities such as those mentioned above with the aim, on one hand, to achieve results in terms of protection of personal data equivalent to traditional deletion of personal data and, on the other hand, to be able to evidence the said protection in case of litigation.

With respect to the rectification of personal data, it may be easier to implement a technical solution which would comply with GDPR requirements. For instance, this might simply mean updating the smart contract and having this update properly deployed on the supporting DLT platform, normally in a new block.

2.3.5. Data transfer and implementation of adequate safeguards

Depending on the governing terms and features of the DLT platform, actors involved in the operation of this platform might be located worldwide. When the legislation of a jurisdiction (of a data importer) does not offer a level of data protection deemed equivalent to the one in force in the EU, prior implementation of adequate safeguards to protect data subjects' rights will be required, as a matter of EU law, whether the data access is at the level of a node, a miner, etc. Even a remote access could qualify as a transfer[71]!

Implementing a worldwide data transfer agreement is not a straightforward solution. It requires a prior review of the data protection regime in each and every jurisdiction, with the likely outcome that no personal data should be transferred in certain jurisdictions. An option could be, on one hand, for the governing and operating documents of a DLT platform to prevent the involvement of nodes or miners located and operated under the laws of jurisdictions deemed inadequate

[71] See the FAQ released by the EDPB further to the Schrems II court decision https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf (accessed on 24 March 2021).

from a European data protection standpoint and, on the other hand, the implementation of some of the transfer mechanisms contemplated in Chapter V of the GDPR. However, implementing such mechanisms might be easier for private or permissioned blockchains than for public ones[72].

To sum up, if written correctly, a smart contract – and notably the information fed and stored on the DLT via such a smart contract – could comply with the GDPR principles and requirements if competent European data protection authorities and courts take a technology neutral approach. Such an approach should focus on the outcome and the level of protection offered to individuals by smart contracts features. As of today, discussions are still taking place at the EU level regarding the requirement a hash function should fulfil in order to qualify as an anonymisation technique, and not simply as a pseudonymisation technique. These discussions also include measures to be implemented to prevent re-identification, such as key reuse encryption or reusable or single-use salt models.

Adopting a cautious approach that takes into account best market practices is therefore advisable. This may require a detailed review of the roles and responsibilities of the various parties involved in the design, the development and the implementation of smart contracts as well as their supporting DLT platforms.

[72] See the paper issued by the French CNIL mentioned in footnote 69.

3. New horizons

Legal challenges will not be the only hurdles to a broader deployment and use of smart contracts and, more generally, of the DLT technology supporting them. Philosophical, political and socio-economic issues and implications need to be dealt with, as smart contracts open up windows to new horizons and new use of code and algorithms in the cyberspace.

Several changes to our current political model are foreseeable. A key one could be a change to our current political and governance models. The increased reliance on code-based decisions instead of on human decisions, could lead to a reduced place left to trust between individuals in our societies, to the benefit of technology and numbers and to the benefit of those controlling them[73]. In this respect, the famous article "Code is law" published by Lawrence Lessig in the Harvard magazine already raised interesting questions, that still resonate today, about the design of code[74]. Lessig purported that, if left unchecked, the code may end up regulating *de facto* human activities and the architecture of cyberspace, with potentially huge consequences on the values of our societies. Similar discussions are taking place within the EU, regarding compliance with ethics and fundamental rights in the context of new technologies.

New horizons and various challenges brought by digital developments in general and smart contracts in particular thus give food for thought. Each of us may wish to think of what this fundamental change means for us, for our children, for our societies, and for the very possibility of a human future in a digital world.

Trust for instance has been a cornerstone to human societies and in particular to contracting and development of smart contracts may lead to a shift here from our trust in humans to our trust in technology.

One might also wonder whether smart contracts could ultimately shape our behaviour at scale, in a sort of human-machine system, and this could prompt us to abandon some of our current silos attitudes and actively build bridges between various disciplines and force us to closely collaborate to build and use technology to support agreed values, if we can see the benefits of such approach for all of us.

3.1 Smart contracts and territoriality of law

Smart contracts and the underlying DLT necessarily raise numerous questions on the territorial application of national legal systems. Such questions are not only linked to the distributed nature of the DLT, but also relate to issues like ethics,

[73] Alain Supiot, La gouvernance par les nombres, Editions Fayard/Pluriel, 2020.

[74] Lessig L., Code is Law, On Liberty in Cyberspace, Harvard Magazine, https://harvardmagazine.com/2000/01/code-is-law-html (accessed on 4 February 2021).

trust, liability and recognition (both legally and operationally) of completely automated processes which may have local implications. Solving them will require cooperation between all the jurisdictions involved in order to achieve a mutually acceptable solution. Considering that discussions regarding the Internet and the use of cloud are still ongoing, there might still be a long way to go before the signature of an international convention addressing these matters.

Smart contracts could create a *de facto* universal mode of dealing upfront with some legal issues, no matter the jurisdictions involved and their respective legal traditions, be they ruled according to the Common Law or to the Roman Law. They may alter the traditional territoriality of law and current solutions in place to handle conflicts of law and jurisdictions, even if they are simply used for partial execution of a more traditional contract and not necessarily a contractual means to settle disputes, especially when they are supported by a DLT platform involving players located across the globe.

Beyond smart contracts, widespread and ever-growing cross-border digitisation has led to a dichotomy between the economic space and the geographical space. For example, one can find himself/herself closer in business terms – hence in the economic space – to people working in Japan for instance than to his/her own neighbour – here in his/her geographical space.

This dichotomy must be accounted for in addressing changes that may need to be brought to national and international private and public laws as it will have consequences on application and suitability of laws and regulations and more generally on our current society model. We may also wish to remember that technological developments have shaped our way of living and even thinking over time. Just think how far we can sometimes live from our place of work thanks to cars and public transportation.

An important element to keep in mind is that digital can take many forms depending upon the social and economic logics that bring it to life. It is obviously time to refresh our ideas about the ways that our society is organised in order to encompass the new digital means of production and to rebalance the relationships between all the stakeholders of our economies and societies. The beauty is that decentralised systems can enable the creation of more agile and less fragile types of systems where power and decision-making are distributed among the stakeholders rather than concentrated in just a few hands, generally called DAOs[75]. The key is certainly not to create a new nation-wide institution or law, or a new international administration, but rather to begin with local institutions that would foster a diverse coalition that learns from each other and constantly adapts.

[75] For more information, you may wish to refer to a European study available at https://blogs.ec.europa.eu/eupolicylab/tag/decentralised-autonomous-organisations/ (last accessed on 31 March 2021).

This White Paper aims at contributing, from the Luxembourg perspective, to such a coalition.

Certainly smart contracts present a number of advantages for (the execution of) contracts, which can easily be translated into code[76].

3.2 Smart Contracts and trust

Blockchain and DLT platforms are often referred to as trustless environments, because no single trusted third party needs to be involved in the operation of such platforms and in the transactions they support. Nevertheless, adoption of smart contracts at scale will require trust, and this, at two levels at least: (i) trust in the underlying technology and the persons implementing and operating it and, (ii) trust in the legally binding aspect of such contracts.

With regard to the underlying technology, building trust will take time, as it is almost always the case for any potential disruptive technology. Let's just think of the history of the Internet for example or, more recently, the development of applications hosted on clouds. Who was keen to store his/her pictures or videos somewhere else than on his/her own computer or external hard drive 10 to 15 years ago?

With regard to the legally binding aspect of smart contracts, attention should be paid to the very fact that, with smart contracts, the word *trust* seems to be prevailing over the word *confidence*. Though both words are similar and mostly used indifferently in English, they do not really have the same meaning.

Trust derives from an old English word meaning "strong," whereas confidence comes from Latin *fides*, literally meaning a person of her word.

Traditional contracting relies on confidence. The assumption of each party is that the other one will respect his/her commitments. Such respect was and is still based on a moral obligation for the parties before becoming a legal obligation

[76] One may in particular argue that automation is a considerable advantage for certain contractual parties in financial transactions, including lenders and more generally secured parties, benefitting from a security created in accordance with the Luxembourg law of 5 August 2005 on financial collateral arrangements, as enforcement of such security may be entirely automated, notably in a context where the secured assets are of digital/dematerialised nature.

enforceable in court. From a broader perspective, confidence can be seen as the cornerstone of human relationships.

Smart contracting is different, at least from a blockchain perspective. There is no need for moral obligation. The deal is not based on the words of the respective parties, but on their ability to comply with the code or the mathematical rules of the algorithm used to translate their words into a smart contract or the contemplated transaction (when the smart contract aims to also be a legal one). Satoshi Nakamoto, in his white paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*,[77] mentions the concept of trust and eludes the word confidence.

To have trust, there is a need to ensure that the architecture on which DLT technology and smart contracts rely are not opaque and can still be understood by humans if need be. In addition, they might also be aligned with the values we, as humans and part of a society, want to abide by and which are reflected in our conventional and constitutional principles, such as the Luxembourg Constitution and the European Convention of Human Rights.

Auditing algorithms will be critical here too, but not necessarily from the same angle: The audit should show that the data needed for a smart contract and relevant algorithms do not lead to discrimination or other breaches of fundamental rights!

3.3 Smart Contracts as a "human-machine system"

A traditional written legal contract can capture various facts and obligations unlike any smart contract which is ultimately a mathematical algorithm. With a smart contract, it is hence only possible to automate the enforcement of a certain number of the clauses of a traditional legal contract. Smart contracts cannot thus currently replace traditional contracts, at least from the point of view of the substance of purely legal clauses open to interpretation, such as liability clauses, handling of unforeseen events or *force majeure*. As an example drawn from our current lives, handling the effects of a pandemic such as Covid-19 could not be captured by a smart contract and its underlying algorithm, unless it can be translated in code as described hereafter.

As of today, with a smart contract, it is only possible to represent direct actions (e.g. reimbursement, cancellation, fine, etc.) in an event-driven mode, i.e. actions are triggered by an X or Y event/report. Here is an example: If event X occurs then Bob must be reimbursed for 20% of the contract, to which he is a party. Thus, the smart contract is, for the time being, primarily on top of a traditional

[77] https://bitcoin.org/bitcoin.pdf.

written legal contract and therefore complementary to such a contract. It is in this respect a human-machine system.

A key element of this design paradigm is testing[78]. To make sure that such a complex human-machine system would work, extensive testing, field piloting, and evaluation are required. Testing always begins with a simulation of key components (here for instance, the algorithms), then the entire system, and concludes with pilot deployments by representative communities as an experiment in which participants give informed consent. Moreover, this testing and evaluation is not just part of the creation of the smart contract, it must also happen continuously after a large-scale deployment of the system. In particular, as circumstances may evolve during the life of the smart contract, it would be necessary to monitor, and in order to adapt, the system must continue to evolve and be reengineered.

3.4 Building a bridge between the legal and the cyber/ IT worlds

Smart contracting has been opening new horizons. Far from being a mere automation of contracts, it challenges the very basis of our legal system and raises

[78] Testing here is a machine learning process: the more algorithms test situations, the more they learn and the more "clever" - and hence useful - they get. While we are currently far from such a scenario, one can thus imagine that at some point, experience gained from this learning process could allow algorithms to behave like some human actors with respect to the enforcement of contracts, i.e. to judge on experience or be the main source used for decision making.

queries as to the place of algorithms and code in our current decision-making process, at any level[79].

This will bring good news despite the challenges and discomfort associated with any significant new developments. For instance, for the investment fund industry, partially automated decisions may prove more rapid, sometimes fairer than the traditional ones. More generally, smart contracting might reduce over-lawyered language, opaque procedures, and written legal clauses and templates that, more often, none (including lawyers themselves) understand. It shall open the door to automated legal acts, where human intervention is reduced to the minimum and where numerical language prevails over natural language. It thus requires a better understanding by all stakeholders that the human factor still lies behind computers and applications and that numerical language may also have its own limits.

No matter how far we go in that direction in the future, this should lead to a shift in the way IT is handled by companies, IT departments being so far merely seen as a support service which could be outsourced. For example, law firms and legal departments of large companies are currently realising how critical and strategic IT can be when it relates to the provision of legal services. The legal profession has the opportunity to transition from being a cost centre and a source of friction, to a centre for new business and opportunity creation. LegalTech tools contribute to the standardisation of a huge proportion of standard legal work. They also facilitate access to the massive amount of legal data accumulated over years. This data can be laws and regulations, such as court cases, legal doctrine, etc. The French Bar of Paris has even set up its own legal tech incubator[80]. These LegalTech companies could facilitate access to law by each of us, as they are offering an on-demand and immediate service. How to ensure that such service offers an adequate level of quality and that it is not biased will be some of the key challenges to be addressed.

Things may be taken one step further. For instance, the ever-growing use of technology in finance is increasingly putting pressure on regulators to shift from regulations that are designed to control human behaviour to regulation that aims to supervise automated processes as well as human behaviour. Regulatory technologies (RegTech) are therefore shaping the future of regulation and might foster regulation by design, i.e. regulatory restrictions embedded technologically in the products. This means that (IT) engineers will now be playing a central role, for instance, in all legal, financial and corporate activities, not only by

[79] Sonia Desmoulins-Canseiler et Daniel Le Métayer, Décider avec les algorithmes - Quelle place pour l'Homme, quelle place pour le droit?, Editions Dalloz, 2020.

[80] https://incubateur-ibp.com/ (accessed on 24 March 2021).

implementing decisions made by lawyers, but also by defining the overall strategy in these activities.

Luxembourg should therefore seek to create an engineering culture of its own that would keep in mind its fundamental political and social values. The Grand-Duchy of Luxembourg may become a haven, not just for young lawyers, but also for young engineers willing to actively contribute to a digital society aligned to these values. It should therefore consider training its own engineers, at the University of Luxembourg as well as in specialised schools of engineering. Teaching them the fundamental values underlying Luxembourg and EU legal systems could help factor them in when developing, implementing or reviewing IT applications and architecture. Luxembourg's education system should still play an essential role in the design and development of the architecture of the digital world.

The culture of design and engineering could be extended to all legal curricula and professions. Legal thinking will remain important indeed, but understanding legal technology, design and engineering should become more and more critical. With the growing momentum of smart contracting, lawyers and judges are more and more likely to face disputes concerning algorithms and coding.

The best protection (from a legal perspective) will potentially not stem from the sole written provisions contained in the relevant legal terms and conditions, but will also have to be built in the product or service's technological design. This will trigger a need for lawyers and IT engineers to work more closely and understand each other to offer upfront adequate joint solutions to their clients. In case of litigation, judges will have not only to understand the legal aspects, but be able to grasp the potential legal implications associated with the use of technological measures and their limits, if any, so they can base their decision on all relevant circumstances.

There will thus be a growing need of lawyers and judges who are tech-savvy so as to be able to communicate and collaborate with IT engineers and developers behind the smart contracts and their support.

APPENDICES

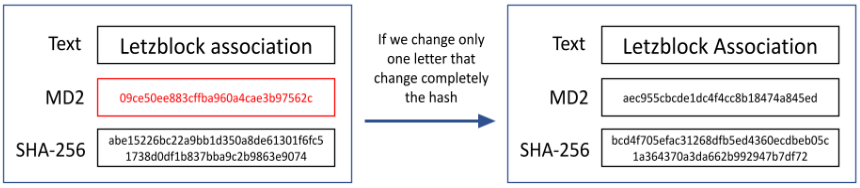
Appendix 1

A Hash example

How to put a document or a private information in the blockchain ?

1) Pass the document or information in a hash function

As a reminder, a hash function is a one way function i.e from the output is not possible to retrieve the input. Furthermore one input give always the same output and two different input can't give the same output. Find bellow an example with two hash functions : MD2 and SHA-256.



Text	Letzblock association
MD2	09ce50ee883cffba960a4cae3b97562c
SHA-256	abe15226bc22a9bb1d350a8de61301f6fc5 1738d0df1b837bba9c2b9863e9074

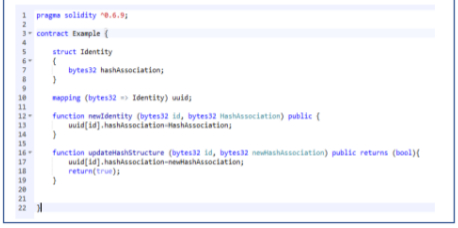
If we change only one letter that change completely the hash

Text	Letzblock Association
MD2	aec955cbcde1dc4f4cc8b18474a845ed
SHA-256	bcd4f705efac31268dfb5ed4360ecdbeb05c 1a364370a3da662b992947b7df72

For the rest of the example we'll use the hash in red.

2) Put the hash in the dedicated function in the smart contract and execute the transaction

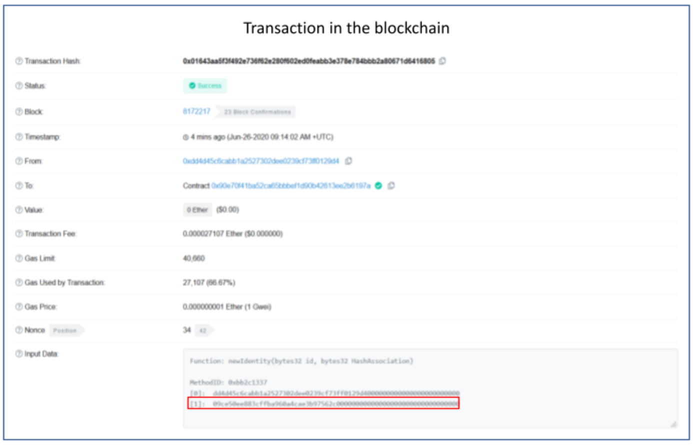
Smart-contract which allows to map an id (public address) with the hash of an association



```
pragma solidity ^0.6.9;

contract Example {

    struct Identity
    {
        bytes32 hashAssociation;
    }

    mapping (bytes32 => Identity) uuid;

    function newIdentity (bytes32 id, bytes32 HashAssociation) public {
        uuid[id].hashAssociation=HashAssociation;
    }

    function updateHashStructure (bytes32 id, bytes32 newHashAssociation) public returns (bool){
        uuid[id].hashAssociation=newHashAssociation;
        return(true);
    }


}
```

3) Check your transaction, you can see the hash in the blockchain

Transaction in the blockchain



Transaction Hash:	0x01643aa5f3f492e736f62e280f602ed0feabb3e378e784bbb2a80671d6416805
Status:	Success
Block:	8172217 23 Block Confirmations
Timestamp:	4 mins ago (Jun-26-2020 09:14:02 AM +UTC)
From:	0xdd4d45c6cabb1a2527302dee0239cf73ff0129d4
To:	Contract 0x90e70f41ba52ca65bbbef1d90b42613ee2b6197a
Value:	0 Ether ($0.00)
Transaction Fee:	0.000027107 Ether ($0.000000)
Gas Limit:	40,660
Gas Used by Transaction:	27,107 (66.67%)
Gas Price:	0.000000001 Ether (1 Gwei)
Nonce Position	34 42
Input Data:	Function: newIdentity(bytes32 id, bytes32 HashAssociation) MethodID: 0xbb2c1337 [0]: dd4d45c6cabb1a2527302dee0239cf73ff0129d4000000000000000000000000 [1]: 09ce50ee883cffba960a4cae3b97562c00000000000000000000000000000000

Appendix 2

The Glossary

This glossary contains a baseline set of definitions of terms commonly used with reference to smart contracts. These definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity or references to the reader.

Algorithm means a procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation.

Note: The word algorithm comes from Arabic Persian mathematician Al-Khawarizmi, the founder of the concept of algebra, who wrote a treatise in 825 on the Hindu–Arabic numeral system which, as translated into Latin, became *Dixit Algorizmi* ('Thus spake Al-Khwarizmi'). His name was then latinized as *algorismus* and later mixed with the greek word *rithmos* (meaning number) to become algorithm as it is now spelled (source Wikipedia, https://en.wikipedia.org/wiki/Algorithm).

Anonymisation involves techniques that can be used to convert personal data into anonymised data and which meet the requirements issued at European and Luxembourg legal and regulatory level to achieve proper anonymisation.

Note: Anonymised data no longer relates to identifiable persons or cannot allow data subject to be re-identified.

Append-only data structure means a property of data storage that allows new data to be appended to the storage, but the existing data is immutable.

Note: The advantage of append-only storage is that the database is immutable and keeps an entire history of all the transactions that have been done.

Artificial Intelligence (AI) means a collection of technologies that combine data, algorithms and computing power.

Note: AI is described as applying learning processes to vast sets of data with the goal of making predictions and classification for e.g. of who is more likely to buy something, to view something, to suffer some kind of illness and even engage in criminal behaviour.

Asset means any valuable right, service, skill or thing which can be traded and more generally any representation of value.

Note: Assets can be physical and tangible or digital and intangible. A physical asset can be tokenized in order to be traded in a digitalised environment.

Assurance (see Audit below).

Audit

- ex ante (or assurance) means a third party expert ensures, before their implementation on the blockchain, that the codes/algorithms underlying a smart contract adequately capture the agreement of the parties.
- ex post (or forensic examination) means a third party expert, in case of litigation related to the proper execution of a smart contract, evidences the suitability or not of the codes/algorithms in translating the intentions of the parties to the agreement.

Automation means the technique, method, or system of operating or controlling a process by reducing human intervention to a minimum.

Binary language (or code) means a mathematical language relying on a base-2 number system and used by computers.

Bitcoin is a crypto-currency initiated in 2008 through a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* written by an unknown author, Satoshi Nakamoto, available online at bitcoin.org/bitcoin.pdf.

As described in the abstract of the paper, Bitcoin is "a purely peer-to-peer version of electronic cash (that) would allow online payments to be sent directly from one party to another without going through a financial institution."

New transactions (or payments) are packaged into a block. This block is then checked and approved by the nodes of a peer-to-peer network through an algorithmic process (*Proof of Work*) and inserted into the chain containing all other previous blocks (namely the *chain of blocks* or *blockchain*). This is the so-called *consensus protocol*.

This allows to avoid double payment and to keep an updated and irreversible public history of all transactions.

Bitcoin has become so popular and powerful that its value has been skyrocketing over the past few years and financial institutions as well as Wall Street have been looking into it.

Besides, concepts stemming from Bitcoin - such as the blockchain and ledger (see definitions below) - are now widely used in the financial industry and beyond.

Block means an individual data unit of a blockchain, composed of a collection of transactions and a block header.

Block header means a data structure that includes a cryptographic link to the previous block.

Blockchain means a technology that allows to record assets, transfer value and track transactions in a decentralized manner, ensuring the transparency, integrity and traceability of data without a central authority to authenticate the information.

- Public (permissionless) means that the systems operate on public domain software and allow anyone who downloads and runs the software to participate

- Private (permissioned) means that the system is essentially a private network where data authorization depends upon the agreement of multiple predefined servers

Note: the concept of blockchain stems from the Bitcoin (see definition above) even though the very word does not appear in Satoshi Nakamoto's paper, Satoshi referring only to a *chain of blocks.*

Boolean logic means operation with binary input and output variables.

Note: Boolean algebra was named after British mathematician George Boole (1815 - 1864) who managed to convert logical reasoning - as first conceived by Aristotle, and further developed by Leibniz -, into binary operations. He thus paved the way to automated reasoning, which is the cornerstone of modern computing.

Code (of law) means a consolidation in a structured manner of various laws and regulations relating to a specific area of law, such as the Luxembourg civil code or the Luxembourg penal code.

Code (computer science meaning) means program instructions.

Note: more generally, code means a set of rules defining a one-to-one correspondence between information and its representation by characters, symbols or signal elements.

Contract (legal acceptation) means a legally binding agreement (written or oral) between one or more parties that create mutual obligations enforceable by law.

Note: Under Civil law, the following basic requirements shall be fulfil for an agreement to be legally binding: (i) the consent of the party who obligates herself, (ii) the party's capacity to contract, (iii) a definite object that forms the subject matter of the engagement and, (iv) a licit cause for the obligation.

Controller (of data) means the person/entity that determines the purposes for which and the means by which personal data is processed (*cf*. Article 4 GDPR).

Note: If a person/organisation decides 'why' and 'how' the personal data should be processed, it is the data controller.

Cryptography embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation and/or prevent its unauthorised use.

Data means representation of information in a formalized manner suitable for human or automatic processing.

Database means a collection of data organized according to a conceptual structure or an entity that stores users and/or network information.

Data processing means systematic performance of operations upon data.

Note: When it relates to personal data, the specific and broad definition of the GDPR (Article 4) shall be used.

Decentralized autonomous organization (DAO) means a digital entity that manages assets and operates autonomously in a decentralized system, but also relies on individuals tasked to perform certain functions that the automaton itself cannot.

Digital assets means a digital representation of value or rights which may be transferred and stored electronically.

eIDAS Regulation means the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification, accessed on 25 November 2020).

Distributed ledger technology (DLT) refers to the processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes.

Note: the concept of DLT stems from the Bitcoin (see definition above) even though the very word does not appear in Satoshi Nakamoto's paper, Satoshi referring instead to *a public history of transactions.*

Encryption means a function used to transform data so as to hide its information content to prevent its unauthorized use.

Ethereum means a decentralized, open-source blockchain featuring smart contract functionality.

Ethereum was initially conceived as an alternative network to Bitcoin, still based on a consensus protocol but with additional functionalities. Beyond transactions, Ethereum enables advanced scripting, which makes it an adequate backbone for blockchain-based smart contracts.

Ethereum was launched in 2015 following an initial white paper written by Vitalik Buterin in 2013. But contrary to Satoshi Nakamoto - the Bitcoin's founder - whose identity has not been disclosed to this day, Buterin is much less secretive. He is well-known worldwide and active on social media.

Framework agreement means pre-existing legally binding agreement between parties to a smart contract.

Function (in computer programming) means a subprogram that returns a value.

GDPR means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN accessed on 22 January 2021).

Hash (function) means an algorithm that transforms large random size data to small fixed size data. The data output of the algorithm is called the hash value.

Note: Hash functions operate in a one-way manner, which means that it is impossible to compute the input from a particular output. A hash might also be a proof of authenticity of a document or a smart contract stored on the blockchain.

Immutable means a property of blockchain and distributed ledger technologies that ledger records can only be added, but not removed or modified, and are designed not to allow changes to historical data over time.

Language means any structured system of communication between humans and/or systems of information (mainly computers nowadays).

- Code (see definition above).
- Natural language consists of words and related letters and symbols, sounds and grammar.

Ledger means information store that keeps final and definitive (immutable) records of transactions.

Node means device or process that participates in a distributed ledger/blockchain network.

Note: Nodes can store a complete or partial replica of the distributed ledger.

Offchain means related to a blockchain system, but located, performed or run outside that blockchain or DLT system.

Onchain means located, performed or run inside a blockchain or DLT system.

Open source means a source code that is released under a license for computer software, but which the copyright holder grants users the rights to use, study as well as the rights to modification and open redistribution subject to specific conditions as applicable.

Oracle means extrinsic data from various data sources which are necessary for the proper performance of a smart contract.

Note: the idea of "oracle" (deriving from the Greek mythology) was introduced in computer science by Alan Turing.

Processor means a person (irrespective of its legal form) which processes personal data on behalf of a Controller (*cf*. Article 4 GDPR).

Protocol means a set of rules governing the exchange or transmission of data between devices.

Pseudonymisation means substituting personally identifiable information (such as an individual's name) with a unique identifier that is not connected to their real-world identity, using techniques such as coding or hashing.

Note: While it can be used to enhance security of personal data, it does not preclude compliance with European data protection requirements.

RegTech means the use of technology in the context of regulation, supervision, monitoring and compliance. It also embraces all the industry, start-ups and businesses that promote such a technology.

Software means an assembly of programs, procedures, rules, documentation and data, pertaining to the operation of an information processing device or system.

Note: initially the word "software" was shaped as an opposite to "hardware", i.e. the electronic components and any other material elements of computers.

Wallet means software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable DLT/Blockchain users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.

Appendix 3

Some technical measures for data protection

The purpose of this appendix is to provide readers with further information on some technical means which entrepreneurs and organisations may want to consider to enhance privacy of the personal data processed via smart contracts and the supporting platforms. To determine the most suitable means, they should take at least into account the principles of privacy by default and by design, their obligation to minimise personal data they collect and the needs and characteristics of their project. It should also be kept in mind that this field is under scrutiny from European data protection authorities as well as the European Union Agency for cybersecurity (the "ENISA") from a security standpoint[81].

For example, the use of salted and peppered hashes may reduce the likelihood of inferring the input value from the output value if the file hash is created using the file and the salt (the salt being the secret information without which the output value may not be recreated). Deleting the hash would allow to break the link between any information or file stored locally and the on-chain hash.

While this may seem like a way to fully anonymise the data, it is doubtful that the data which remains on-chain once the link is broken (i.e. the salted hash) would be deemed anonymous and would not amount to personal data. The Dutch Data Protection Authority has already taken the view that salted hashing is, in principle, personal data.[82]

The use of certain systems may provide built-in security mechanisms protecting the integrity of the data. For example, Ethereum's clique system for validation, which is a Proof of Authority system, allows to maintain a number of full nodes which validate requests, produce blocks and add them to the chain. Full nodes may be added or removed from this list of validators by other full nodes voting on it, thus limiting access to the network. This system is characterised by transparency (since all blocks are visible to all full nodes) and a strong degree of immutability. As a result, the integrity of the data is protected. The use of such system may help with compliance with the GDPR, as: (i) nodes would reject a block containing a unilateral change to the chain, (ii) the use of encryption and hashing for identifiers and transactional data stored on the blockchain is a useful

[81] https://www.enisa.europa.eu/news/enisa-news/enisa-report-on-blockchain-technology-and-security (last accessed on 31 March 2021)

[82] Dutch Data Protection Authority, The data breach notification obligation as laid down in the Dutch Data Protection Act: Policy rules for the application of Article 34a under the Dutch Data Protection Act, 8 December 2015. This paper is available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/policy_rules_data_breach_notification_obligation.pdf (last accessed on 31 March 2021).

security measure which reduces the risk of linking the dataset to the data subject and, (iii) the chain provides an audit trail of who had access to what information at which given time, and who shared data with whom.

However, while using this system makes tampering with the data stored on the chain burdensome and expensive, the risk of tampering cannot be excluded. For example, where 51% of the nodes of the network are colluding, they may implement changes on the chain which do not reflect reality. Moreover, the use of encryption and hashing are not guaranteed to be tamper proof and there continues to exist a risk of "reversibility" (i.e. possibility to reverse the process and reconstitute the original data using e.g. brute force decryption) and "linkability" (i.e. possibility to link the encrypted data to the data subject e.g. by examining patterns of use, the context or by combining other pieces of information available). Further, identifiers and transactional data recorded on the Blockchain may leave traces which, when combined with other identifiers and information, may be used to create profiles of data subjects and allow to identify them.

Appendix 4

Contributors

LëtzBlock would like to warmly thank all the participants who have expressed their interest in smart contracts and contributed to this White Paper.

Anne Baudoin

Etude Marianne Korving, Luxembourg

Commercial lawyer with a significant past experience as in-house lawyer, Anne advises clients on various subjects such as data protection and the new digital trends; Luxembourg company law; commercial law, and investment fund laws (UCITS, AIFM,....

Anne is member of Luxembourg Bar and holds a Doctorate of Law from Paris II University (Institut d'expertise et d'arbitrage de Paris award, 1995).

Monique Bachner

Monique is an Independent Director and Board Advisor, sitting on several Boards and running her own legal advisory practice.

Monique's particular expertise is at the intersection of ethical, governance and regulatory frameworks, and is active in several international working groups related to governance, ethics, digitisation, decentralisation, and regulations.

Boika Deleva

Clifford Chance, Luxembourg

Boika is a member of the Banking, Finance and Capital Markets practice at Clifford Chance's Luxembourg office and a member of the Luxembourg Bar since 2017. Boika specialises in banking and financial services regulation as well as derivatives, finance, securities, insolvency and general banking law matters, with a particular focus on fintech and new technologies.

As part of Clifford Chance's Tech group, being a dynamic cross-practice global team within Clifford Chance, Boika assists both incumbents and start-ups in the financial markets space to meet their tech challenges.

Anthony Favier

Elvinger, Hoss & Prussen, Luxembourg

Anthony became a member of the Paris Bar in 2014. He was admitted to the Luxembourg Bar under his home title in 2015 and joined Elvinger Hoss Prussen in 2017.

Anthony holds a maîtrise in business law from the Université Paris XII (France) and a Master's degree in management des médias from Sciences Po Rennes (France).

He is a lawyer specialized in ICT matters and notably provides legal advice on data protection as applicable to the funds' industry.

Yohan Maurin

PwC, Luxembourg

Yohan is a blockchain developer at PwC Luxembourg and he is active in the Luxembourg blockchain ecosystem. He has worked on various smart-contracts design and development, blockchains architecture and crypto-assets issuance.

Prior to his role at PwC, he was a Blockchain engineer/developer at Liquidshare and Universal reward protocol.

Yohan holds a degree in financial engineering with a blockchain specialization.

Olivier Marquais

Loyens & Loeff, Luxembourg

Olivier Marquais, senior associate, is an attorney-at-law in the Litigation & Risk Management Practice Group of the Luxembourg office of Loyens & Loeff. He focuses on financial and asset management disputes (litigation and arbitration). Olivier's practice includes contract drafting and negotiation, pre-contentious and contentious matters. He has substantial experience advising on, and representing clients in, complex, high value cross-border contracts and disputes.

Vincent-Emmanuel Mathon

Vincent-Emmanuel Mathon is an engineer and a Doctor of Philosophy. He has been leading two parallel careers, one in the Real Estate field as a Property Manager and one in the academic sector, giving lectures and papers for the International Society for Utilitarian Studies and for the *Bentham Project* from the University College of London.

His main interests are the philosophy of green finance and circular economy, together with the philosophy of politics and law and its connections with science and technology.

Roger Tafotie

Adviser to The Blockchain Academy and co-founder of Opexify, Luxembourg

Roger is currently co-founder and Managing Director at Opexify – a Luxembourg based ICT company that specializes in enterprise software development and digital transformation. He is also researcher and advisor at The Blockchain Academy and Adjunct Professor in law at the University of Luxembourg. Prior to co-founding Opexify, he was a lawyer with the Luxembourg Bar and, more recently, an Associate Director with EY Luxembourg.

His main areas of interest include, amongst others, impact innovation and digital transformation.

Roger received a PhD with *summa cum laude* in Law and Economics from the University of Luxembourg.

TABLE OF CONTENT