Blockchain and public procurement

Raquel Carvalho, Ph.D. [*]

Universidade Catolica Portuguesa Faculdade de Direito

rmcarvalho@porto.ucp.pt

Abstract

Public procurement relies in an apparent irreconcilability between competition, which implies some confidentiality, and transparency. The latest Public Procurement Directives have made e-procurement a mandatory feature. Since blockchain technology has been developed and designed to accomplish integrity, transparency, efficiency and data accuracy, goals which are very much appreciated in public procurement, an interesting question then arises: is there room to apply this technology within public procurement procedures? Will smart contracts be an interesting tool within public procurement? Considering public duties such as data protection, which must be complied with by contracting authorities, and some blockchain features such as non- withdrawable information and the likely broad access to the information there enclosed, one can be drawn to conclude that there is no possible conciliation between these two procedures. The mandatory e-procurement implies some neighbouring problems with this technology. Yet, are there any technological solutions for some of the drawbacks?

Keywords

Blockchain; public procurement; e-procurement; smart contracts; personal data; industrial and commercial secrets; award criteria; discretionary decision; software code; law and technology.

1. Introduction

[*] This paper is financially supported by national funds through FCT – Foundation for Science and Technology, IP, within the Project UID/DIR/04859/2013.

Public procurement relies in an apparent irreconcilability between competition, which implies some confidentiality, and transparency. According to recital (2) of Directive 2014/24/EU of the European Parliament and of the Council, 'public procurement plays a key role in the Europe 2020 strategy, set out in the Commission Communication of 3 March 2010 entitled 'Europe 2020, a strategy for smart, sustainable and inclusive growth' ('Europe 2020 strategy for smart, sustainable and inclusive growth'), as one of the market-based instruments to be used to achieve smart, sustainable and inclusive growth while ensuring the most efficient use of public funds'. Hence, public procurers have now some more complex goals to achieve and not only the market goal. Even though the Directives aim to harmonise legal regimes, their implementation varies according to the economic development of each Member State and their inner financial difficulties. These natural differences also make a difference regarding in the engagement in pursuing each additional goal inherent to sustainable procurement, determining the emergence of new tools.

Since Blockchain technology has been developed and designed to accomplish integrity, transparency, efficiency and data accuracy, goals which are very much appreciated in public procurement, we intend to discuss whether there is room for applying this technology within public procurement procedures and whether this will be a better solution when compared to the present ones (section 2). The two main questions addressed in this paper imply thus the discussion of smaller ones. Therefore, after briefly explaining in what Blockchain technology consists, stressing its key features, its advantages and disadvantages (section 2.1.), and addressing the 'smart contract' tool (section 2.2.), we intend to confront Blockchain technology with the electronic platform solutions, identifying common problems.

As the premised framework of the analysis is the EU legal order and the latest Public Procurement Directives have made e-procurement a mandatory feature, we have chosen the Portuguese case of e-procurement implementation because not only does it have high rates of success, but also because it has been dealing with and solving some of the identified problems regarding technology. Hence, the case chosen does not intend to set aside other examples within the EU, but we figured that all Member States have experienced the same difficulties. Additionally, this section's only aim is to help readers understand the technological framework (section 3).

In section 4, bearing in mind the kind of legal requirements made by open public procurement procedure rules (and their legal safeguards regarding data protection, both personal and private), we will address some of the sensitive issues (section 4.1.) concerning the tender presentation, the evaluation phase under the award criteria, the choice of the best valued proposal, the habilitation phase and the contract conclusion. Then, in section 4.2., we will try to understand if those requirements fit the Blockchain way of working, including the 'smart contract' solution. Our goal is to verify if this technology is more adequate and suitable for public procurement than the present solutions of electronic platforms and traditional contract execution. Starting from some usable smart contract solutions, it will be possible to conclude that, although some of the key features of the technology are very welcome in public procurement, a set of difficulties in using this solution remains. Not only when addressing the procedure stage, where the sensitive problems regarding personal and confidential data are more evident, but also in contract execution, due to the general complexity of public contracts. Nevertheless, there is slightly room for a kind of public contracts, particularly if they are concluded under the best price award criterion and the main object is related to supply.

2. The Blockchain technology

2.1. Preliminary remarks

Blockchain began as a database of online transactions, which explains its features, mainly decentralisation and immutability. Nowadays, it is a distributed digital technology designed to accomplish integrity, transparency and efficiency.[1] Blocks of information are constantly added and not redrawn, which can explain, alongside with cryptography, the transparency and accountability features. Once the data is verified through a consensual process by all the people involved (which also allows synchronisation), and then stored on several computers (nodes), it cannot be changed, therefore becoming immutable.[2] It is, therefore, a distributed ledger.[3] It is maintained by an algorithm, so 'the transaction history [is] not to be managed by a central authority' – therefore it is a decentralised database. It aims to 'achieve resilience through replication' – if a computer fails the data is nevertheless preserved.[4] This copy distribution prevents the success of a cyber-attack.

[1] Michèle Finck states that it remains 'in flux' ['Blockchains: Regulating the Unknown', *German Law Journal* 19 (2018) 665 at 667].

[2] Roland Berger, 'Blockchain – A Promising Technology for the Belgian Public Administration'. 2018. Retrieved 8 October 2018 https://www.rolandberger.com/en/Publications/Blockchain.html.

'When a block is verified as 'true and trustworthy' via the consensus protocol, it is posted practically simultaneously to each consortium member's copy of the distributed ledger. Each ledger has a unique *hash Key* calculated based on the precise content of all the transactions in the block' (Jason Killmeyer, Mark White, Bruce Chew, 'Will Blockchain Transform the Public Sector? Blockchain Basics for Government', Deloitte Report https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf). Nevertheless, Michèle Finck stresses that the immutability feature should be understood as such as far as there is no human intervention (Finck 'Blockchains: Regulating the Unknown' (n 1), 665 at 668). See also, Angela Walsh, 'The Path of the Blockchain Lexicon (and the Law)', *Review of Banking & Financial Law* 36 (2017) 713 at 735 ff). Kevin Werbach, when addressing the security issues and the trust in smart contracts, also discusses the immutability in Ethereum ('Trust, but Verify: Why the Blockchain Needs the Law', *Berkeley Technology Law Journal* 33 (2018) 490 at 517. Available at https://ssrn.com/abstract=2844409).

Primavera Di Filippi and Aaron Wright, addressing the tamper-resistant feature, inform that it is possible, within Blockchain technology, 'to determine whether a party is entitled to view, share, or modify data. Such an approach is already being explored in the context of health data and electronic medical records' [*Blockchain and the Law – The Rule of Code* (Cambridge, Massachusetts, London, England: Harvard University Press, 2018) 112].

[3] Mark Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective, *Computer Law & Security Report* (June 2017) 1 at 3.

Angela Walsh discusses whether blockchain is in fact a distributed ledger. Walsh, 'The Path of the Blockchain Lexicon (and the Law)' (n 2), 713 at 765.

[4] Michèle Finck and Valentina Moscon, 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0', *IIC – International Review of Intellectual Property*

Additionally, each modification is spotted by all participants, which prevents unauthorised modifications.[5]

Hence, it relies upon a chain of information which validates the existence and accuracy of the information provided in the distinct stages – the technology does not assure information quality, only the procedure accuracy. Trust is built upon the agreement of all the parties in the Blockchain to abide by the same protocol, which is why there are different moments and parties in the validation process.[6] And the entire process is guaranteed by data encryption. Therefore, the inner accuracy of the information is a different question, because the truthfulness that can be guaranteed by Blockchain technology only goes as far as the kind of process used, not the inner truthfulness and accuracy of the information stored. This technology cannot solve any problems regarding untruthfulness, but it can exacerbate them as it is in general difficult to delete or change information (even if, in some cases, it is possible to have permissions to change or delete information).[7]

The range of participants embraces transparency and ideally underpins efficiency. The 'cutting out [of] intermediaries'[8] and the automation process improve financial efficiency through the reduction in administrative costs.[9] Mark Giancaspro, reflecting upon smart contracts, also refers to the promised efficiency linked to the fact that they do not need

and Competition Law 50(1) (2019) 77 at 89; Michèle Finck, *Blockchain, Regulation and Governance in Europe* (Cambridge University Press, 2019) 7.

[5] Finck 'Blockchains: Regulating the Unknown' (n 1) 665 at 670.

[6] As Michèle Finck says, '*consensus protocols* provide consistency among the many copies of the ledger'. The protocols are the 'source of trust in the system' (Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 19-20). At least, the accuracy of gathering data but not inner accuracy. See *infra.*

Trust is a very valuable asset: 'it creates reserves of goodwill that facilitate social interactions and business transactions', Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge, Massachusetts, London, England, 2018) 19. However, this trust is related to the whole system (*ibid* 96).

[7] Referring to these issues, Primavera Di Filippi and Aaron Wright, *Blockchain and the Law – The Rule of Code* (n 2) 114 ff.

[8] Berger, 'Blockchain – A Promising Technology for the Belgian Public Administration' (n 2).

[9] Mark Giancaspro gives the example of the 'contract formed via credit card purchase' that, if the Blockchain technology is used, the transactions costs are completely avoided (Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective' (n 3) 1 at 5).

the usual intermediaries such as banks, insurance companies, and so on: 'this process of disintermediation improves efficiency by allowing the Blockchain to address all critical aspects of the transaction from record-keeping to auditing, monitoring and enforcement'.[10] This kind of efficiency can be embraced in the contractual process as referred by Merit Kõlvart, Margus Poola, and Addi Rull, which includes an 'overview of the past behaviour of contracting parties.'[11]

Despite the above-mentioned advantages regarding efficiency, some difficulties have been identified: the inefficiency by design, high-energy consumption, the need to be upgraded in order to be functional at scale, and the technical limitations. These features seem to compel us to be cautious when embracing the technology: Blockchain is mainly technology the building of which is ongoing.[12]

Both Blockchain's governance and configuration vary. In fact, it seems more of 'a class of technologies' rather than one single technology.[13] The main distinction is between public (permissionless) and private (permissioned) blockchains.[14] As opposed to private blockchains, public blockchains involve several information holders. Public blockchains usually have no network access control, and no gatekeeper, since this technology was created without specific access controls from the beginning.[15] Accordingly, to Michèle Finck and Valentina Moscon, 'on such ledgers, transactions are publicly auditable, which ensures transparency but minimizes privacy.'[16] Bearing in mind some of public procurement features, at least during procedure, we could think that a permissioned

[10] *Ibid* 4.
[11] Merit Kõlvart, Margus Poola, and Addi Rull, 'Smart contracts', in: Tanel Kerikma¨e and Addi Rull (eds) *The Future of Law and eTechnologies* (Springer, 2016) 134.
[12] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 1-2.
[13] Roman Beck, Christoph Müller-Bloch and John Leslie King, 'Governance in the Blockchain Economy: A Framework and Research Agenda' (Working paper), *Journal of the Association for Information Systems* 9(10) (2018) 1020 at 1021.
[14] There are also hybrid forms of blockchains.
[15] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 14.
[16] *Ibid* 90. Regarding the privacy issues, see Finck, *ibid* 88-116.

solution wold be a better hypothesis to consider. On the other hand, after the period of information containment, there are some transparency obligations. And even at the beginning of the procedure, when considering an open procedure, access should be open to all possible economic operators.[17]

In the meantime, though, some Blockchain experiences have been implementing control tools. Concerning private blockchain solutions, there is some network access control. Yet, the traditional control of local networks such as firewalls and virtual private networks may not be enough to achieve the security level expected from such technology.

Nevertheless, as the Deloitte Report states, 'blockchain can provide advanced security controls, for example, leveraging the public key infrastructure (PKI) to authenticate and authorise parties, and encrypt their communications'.[18] Encryption requires a private key to allow access to the information. And this key is another security measure alongside encryption: when I store information in this technology, it only can be accessed by whom I give permission to. So, I maintain the sovereignty upon my data, which is a common goal with GDPR.[19]/[20] When gathering decentralised, sequential hashing and

[17] At the beginning of an open procedure, the contracting authority does not know how many economic operators will be presenting a tender, nor their identity.

[18] 'PKI is a set of roles, policies, and procedures required to create, manage, use, store, and revoke digital certificates and manage public-key encryption', Eric Piscini, David Dalton, Lory Kehoe. 'Blockchain & Cyber Security. Let's Discuss'. Retrieved 9 October 2018 https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf. Michèle Finck recognises public Key infrastructure (PKI) and has as two important cryptographic tools (Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 28).

Describing the functioning of the private key, Michèle Finck, 'Blockchain and Data Protection in the European Union', *Max Planck Institute for Innovation and Competition Research Paper Series* 18-01 (2018) 1 at 4 ff.

[19] See Article 20. We are addressing only one type of personal data: that is enshrined in the object of the transaction. However, the Blockchain embodies also metadata, which can also be considered personal data (the sender's and recipient's addresses and a timestamp can be considered as such, as the blockchain's users are natural persons).

[20] The General Data Protection Regulation (GDPR), 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, and repealing Directive 95/46/EC, has a scope of application. Our reflection is made under the premise of Member States of EU that are obliged under Public Procurement rules and therefore also under the scope of GDPR.

cryptography, this system makes it quite difficult for anyone to tamper with information when you consider the main alternative of a database.[21] Therefore, this private key serves at least one of the goals of data protection and data confidentiality and fulfils the requirements of authentication and authorisation.[22] But as Kevin Werbach expressly states, 'Blockchain-based systems are vulnerable'.[23] Perhaps in a smaller degree regarding the Bitcoin solution, but higher in other Blockchain-basis solutions.

Hence, there are still some risks, even when these security measures are deployed. There are user-related risks and code risks.

Regarding user-related risks, at least two kinds of risks can be identified: the one of the key being stolen and those inherent to accessing networks from several computers.[24] Key safeguard is important regarding cryptography and security.[25] Although there are already powerful computers running 24/7 to break codes, it is very likely that in the future much more powerful computers – quantum computers – can achieve the break in lesser time.[26] So, even if I neither lose my key nor is it stolen, the technological risks exist.[27] The other user security-related question, this one regarding the user behaviour, concerns the access

[21] In this sense, Piscini, Dalton, Kehoe 'Blockchain & Cyber Security. Let's Discuss' 7. As Michèle Finck explains, 'through this process, data is chronologically ordered in a manner that makes it difficult to tamper with information without altering subsequent blocks', Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 4. Data is trendily unaltered as a 'collusion between the majority of the network's nodes' could in fact alter the data (*ibid* 4).

[22] Data protection is not the only problem related to blockchain technology. Privacy is another one and both of them 'are two different concepts (but they are rights)', Nicola Fabiano, 'The Internet of Things ecosystem: the Blockchain and Data Protection Issues', *Advances in Science, Technology and Engineering Systems Journal* 3(2) (2018) 5.

[23] Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (n 2) 490 at 515. Primavera Di Filippi and Aaron Wright also acknowledge that, although being resilient, this technology is not 'immutable and can be attacked and manipulated by malicious parties' (*Blockchain and the Law – The Rule of Code* (n 2) 113); also Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 30.

[24] Referring precisely the 'theft or disclosure of a private key', Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 114.

[25] Addressing this issue, within Bitcoin solution, Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward William Felten, 'SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies", in: *Proceedings of the 36th Ieee Symposium on Security and Privacy* (2015) p. 104.

[26] For instance, there are some flaws regarding the random numbers generators.

[27] Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (n 2) 490 at 515.

from different computers. This kind of access adds another security issue, increasing both the possibility of breaking the code and the chances to steal the key.

Beyond these security issues, there are also inner code risks. It is known that the technology (Bitcoin code) has code bugs and the inventor's (Nakamoto's) solution regarding this issue 'is remarkably robust, but it can be overcome by a 51% attack'.[28] Regarding the public Blockchain, the most used consensus method is the *proof-of-work*: 'nodes contribute computing power to secure and maintain the system and engage in an economic competition (…) before they can propose a valid block to the nodes'.[29] Each miner has to solve a puzzle and, when they reach the solution, that is seen as a proof of good faith 'since it requires the miner to invest resources (CPU power and electricity) into updating the ledger. Nodes will only accept blocks which contain the solution to the puzzle.'[30] This method implies an investment in energy and computational resources. Due to the excessive cost involved in this proof, *mining pools* – a 'consolidation of miners' – have been appearing, which allows the sharing of both rewards and transaction fees among miners. This solution 'may further undermine the security of the network' and may increase the 'so-called 51% attack'. [31] In order to face some of the problems of this mechanism, other security methods are being tried. One of the new consensus protocols is the *proof-of-stake*: 'participants must show a 'stake' in the system in order to participate in the protocol. An example would be a weighted raffle based on the number of coins

[28] *Ibid* 490 at 515. Addressing the security risks, Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2)113 ff.

[29] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 20. Describing the proof-of-work (PoW) and proof-of-stake (PoS), Lin William Cong and Zhiguo He, 'Blockchain Disruption and Smart Contracts', (December 27, 2018). Available at https://ssrn.com/abstract=2985764 or http://dx.doi.org/10.2139/ssrn.2985764.

This system 'imposes consensus on the precise order of transactions. Nodes are agreeing not just on what happened, but in what sequence it happened'. Werbach, '*The Blockchain and the New Architecture of Trust* (n 6) 64.

[30] For more detailed and technical explanations, see Jean Bacon, Johan David Michels, Christopher Millard and Jatinder Singh, 'Blockchain Demystified'. *Queen Mary School of Law Legal Studies Research Paper* 268 (2017), available at https://ssrn.com/abstract=3091218.

[31] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 21.

held by each participant.'[32] But there are other protocols for distributed ledgers: 'Proof of space, where participants must provide a specified amount of memory to compute the proof, in order to participate in the protocol'; 'Practical Byzantine Fault Tolerance (PBFT), a traditional, synchronous distributed consensus protocol. These protocols have been proved correct and their performance has been evaluated. They have been assumed to operate across a few tens of nodes, for which case they perform well, but they have not been used at large scale'; 'earliest timestamp wins, [that] relies on trusting the timestamp generation hardware in the miners participating in the protocol. A hardware technology called 'roots-of-trust' could be built on'; and 'Hashgraphs [which] have been proposed as an alternative to PBFT for lower overhead and increased scalability'.[33]

What seems to be consensual is that the measures to secure distributed ledgers varies depending on the kind of technological solution[34] and the field business it is applied to (banking sector, health, small commercial businesses and so on).[35]

There are data protection-related issues regarding transparency and its connection with the keys, as a means to protect privacy. Hence, although presented as an advantage, transparency can also become a 'concern'. The existence of private keys does not assure anonymization of the encrypted information because with the right key access to full disclosure is possible. That is why encryption is a pseudonymisation and, under Recital

[32] Bacon, Michels, Millard and Singh, 'Blockchain Demystified' (n 30) 1 at 15; Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 21.

[33] Bacon, Michels, Millard and Singh, 'Blockchain Demystified' (n 30) 1 at 15-16.

[34] 'Permissioned blockchains do not provide the same assurance of non-interference because access is limited to identified parties', Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (n 2) 490 at 516.

[35] Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (n 2) 490 at 517.

26 of GDPR, is qualified as personal data.[36] The risk of reidentifications is real.[37] That is why relying on anonymity to maintain privacy can be misleading in Blockchain as there are techniques that can be used to identify the parties.

Another data protection-related issue about Blockchain as a global decentralised system is the fact that there is no one that can be accountable for the protection of data, not even their owner.[38] The General Data Protection Regulation (GDPR) was designed to deal with personal rights regarding technologies such as clouds, not for decentralised systems such as Blockchain technology.[39] Therefore, apparently, there is a profound incompatibility between the General Data Protection Regulation (GDPR) and Blockchain.[40]

So, features that are very appealing such as transparency and traceability are simultaneously weaknesses when observed from a data protection point of view. For Primavera di Filippi and Aaron Wright, 'the transparency, resilience, and tamper resistance of a blockchain may undermine the effectiveness of these blockchain-based registries and other data management systems, crating security and privacy risks.'[41]

[36] In this sense, Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 10. Explaining some techniques that may overcome this pseudonymisation, *ibid* 11 ff. Javier Wenceslao Ibañez Jiménez points out that anonymity is assured 'through the use of the sophisticated system of double asymmetrical key, grounded in the use of two distinct keys', both public and private [*Derecho de Blockchain y de la Tecnología de Registros Distribuidos* (Aranzadi: Navarra, 2018) 43].
Recital 26 reads as follow: 'Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person'.

[37] Primavera di Filippi and Aaron Wright give the example of the Netflix's dataset deanomysation made by the University of Texas at Austin 'simply by comparing rankings and timestamps with public information available at the IMDB database' (*Blockchain and the Law – The Rule of Code* 116, footnote 43). Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets'. *IEEE Symposium on Security and Privacy (SP)* (2008) https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[38] Michèle Finck explains the possibility of the data subject being, at the same time, data controller regarding their own personal data. Michèle Finck, 'Smart Contracts as a Form of Solely Automated Processing under the GDPR', *Max Planck Institute for Innovation and Competition Research Series*, paper No. 19-01 (January 8, 2019), 6 (http://dx.doi.org/10.2139/ssrn.3311370); in the same sense, Bacon, Michels, Millard and Singh, 'Blockchain Demystified' (n 30) 45.

[39] As Michèle Finck points out, 'whereas the GDPR was fashioned for a world where data is centrally collected, stored, and processed, blockchains decentralize each of these processes', Finck 'Blockchain and Data Protection in the European Union' (n 18) 1 at 1.

[40] Finck 'Blockchain and Data Protection in the European Union' (n 18) 1 at 1.

[41] Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 116.

Another appealing feature of this technology is data immutability, as it grants trust in the information gathered.[42] Yet, one of the downsides of this feature is that information is, at least by principle, non-withdrawable information. This feature can raise a great deal of critical issues. Not only when inaccurate information is stored, but mainly when personal data is.[43] When dealing with personal data, both EU and internal law establish the right to be forgotten and to delete personal information as an imperative feature. Given the fact that the owner of the data can be the data controller as well, they should be aware of this side of immutability. On the other hand, there are already some technical tools that can be used to address this problem: encrypted personal information,[44] only accessed by private keys, can be 'forgotten', when private keys (belonging to the owner of the data) are forgotten, and the information is no longer accessible to or by anyone. Another tool is to write 'the hash of transactions to it, while the transactions themselves are stored outside of the system'.[45]

However, these features that we have been describing have been stressed as key features when Blockchain is related to Bitcoin. Whenever the technology is used for other purposes, the benefits are not always exactly the same. Hanna Halaburda expressly states that it has been 'a challenge to create a decentralized, permissionless and secure blockchain to transfer assets other than a native cryptocurrency'. [46] The author identifies two major difficulties in applying this technology outside Bitcoin: (i) the gateway

[42] For Kevin Werbach, it represents 'the time dimension of blockchain trust', *The Blockchain and the New Architecture of Trust* (n 6) 101.

[43] Personal data is broadly defined in GDPR: 'means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' [Article 4 (1)].

[44] Still considered personal data under EU law, though. So, this kind of information, even encrypted, is subject to GDPR (Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 1).

[45] Piscini, Dalton and Kehoe, 'Blockchain & Cyber Security. Let's Discuss' (n 18) 7.

[46] Hanna Halaburda, 'Blockchain Revolution without the Blockchain' (2018). Retrieved 4 March 2019 https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf.

problem (which does not exist in Bitcoin as it is native): 'whether the gateway is an individual, an institution or a consortium, it needs to be a trusted third party for subsequent users of the blockchain'; (ii) assuring immutability: 'what makes the ledger immutable is the fact that adding a block to the blockchain is costly. (…) The network participants are rewarded for their costly work with bitcoins' – without bitcoins, what could motivate the participants?[47]/[48]

Consequently, people are choosing closed, permissioned Blockchains, which, although parting from the Blockchain technology with bitcoins, are driving away 'because a blockchain without bitcoins is no longer virtually immutable without a trusted third party.'[49]

So, one must conclude that this technology is already beyond its inception – cryptocurrencies – and seen as a new way to do business, even within the public administration.[50] There are already some experiences in Sweden, the Republic of Georgia, the state of Illinois and the Republic of Ghana, regarding real estate transactions;[51]Antwerp, with birth registration; Australia, regarding police evidence from video cameras; the United Arab Emirates, with business registration, and logistics; and

[47] *Ibid*.
[48] Addressing the cost issue of being a miner (the need for 'expensive hardware to mine a new block' and cost energy), Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 21.
[49] Halaburda, 'Blockchain Revolution without the Blockchain' (n 46) 8.
[50] Michèle Finck explains the possible Regulatory Strategies regarding blockchain technology. One of them is the issue of new legislation, pinpointing some examples in Arizona, regarding electronic signatures, Vermont, regarding blockchain evidences admissibility in court, and France, regarding crowdfunding (Finck, 'Blockchains: Regulating the Unknown' (n 1) 665 at 679).
[51] Explaining the 'registries and Public Sector Information', Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 109 ff.

Estonia, with a voting system.[52] So we can foresee that the use of Blockchain will increase within the public sector.[53]

2.2. Smart contracts as a new legal tool?

Blockchain technology is also a 'programmable platform', which enlarges its usefulness beyond data storage. That is the reason why 'smart contracts' are usually related to Blockchain technology.

A smart contract is an agreement that has an automatic execution, usually by computers.[54] Nick Szabo coined the term back in the 1990s, even though the legal concept appeared before Bitcoin.[55]/[56] Michèle Finck stresses that, although there is an excitement around the concept, smart contracts are 'little more than a deterministic if-then relation, it is plain

[52] This is one of the uses of Blockchain technology that relies upon immutability. Discussing the several meanings of the concept and how the feature is set to 'sell' the technology: 'This is why so many see potential for blockchain technology to change systems including voting, government benefits, health records, insurance, and property records, among countless others. With certainty and permanence in our records, no one can cheat anymore, because cheating can always be called out with reliable records, and risks can be assessed more accurately across the board. Certainty and permanence are indeed potent tools, and if we have finally found these with blockchain technology, then it is small wonder that so many are celebrating' (Walsh, 'The Path of the Blockchain Lexicon (and the Law)' (n 2) 713 at 737).

[53] In this sense, Killmeyer, White and Chew, 'Will Blockchain Transform the Public Sector? Blockchain Basics for Government' (n 2) 2. By 2017, there were 117 Initiatives in 26 countries (*ibid* 3). The OECD analysis of data collected by The Illinois Blockchain Initiative (April 2018) shows 203 Blockchain Initiatives in 46 countries. Retrieved 8 December 2018 http://www.oecd.org/parliamentarians/meetings/gpn-meeting-october-2018/OPSI-Blockchain-Presentation-for-Global-Parliamentary-Network.pdf.

[54] As Max Raskin points out, although it is possible to find alternative and broader definitions of smart contracts", for legal purposes, the key feature is the "excision of human control", "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review* 1 (2017) 305 at 309. The most common and old example is the vending machine.

[55] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks', *FIRST MONDAY* 2(9) (1997). Retrieved 23 October 2018 http://ojphi.org/ojs/index.php/fm/article/view/548/469; Tim Swanson, 'Great Chain of Numbers: A Guide to Smart Contracts' S*mart Property and Trustless Asset Management* 67 (2014); Nick Szabo, 'The Idea of Smart Contracts' (1997), retrieved http://szabo.best.vwh.net/smart_contracts_idea.html; Aaron Wright, Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', retrieved http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (2015); Kevin Werbach, Nico Cornell, 'Contracts Ex Machina', *DUKE Law Journal* 67 (2017) 313-381; Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 72 ff.

[56] Ethereum is one of the most important platforms regarding smart contracts.

that they have been a reality long before blockchain technology came along'.[57] Or, if another definition should be given, a 'small computer program that is deployed on a blockchain'.[58] Contract rules are turned into programming language – the creative phase after which the software is frozen 'while being added to the chain'[59] – and it seems, at first glance, that these contracts no longer need 'legal expertise', as the 'payment due for the contract could be executed automatically' and 'without possibility of interference by any party, and without the need of legal enforcement'.[60] This feature is sometimes referred to 'as 'tamper-proof' execution' and this ability to perform 'on its own' is seen as the key that makes the 'contract 'smart''.[61]

But, for Michèle Finck, these 'contracts' are neither smart in 'AI sense (they need outside output to determine real-world events)[62] nor legal contracts'.[63]

There are several examples of smart contracts in the cryptocurrency field, but also, as Michèle Finck states, in 'automatic transfer of collateral in the event of default or to disburse employee compensation if performance goals are achieved', 'InsurTech for

[57] Finck, 'Smart Contracts as a Form of Solely Automated Processing under the GDPR' (n 38) 6. Therefore, the permanent order in bank online to transfer money is a smart contract; also, Halaburda, 'Blockchain Revolution without the Blockchain' (n 46) 5.

[58] Finck and Moscon, 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0' (n 4) 77 at 91.

Nevertheless, it should be noted that smart contracts are not necessarily linked to this technology (Finck and Moscon, 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0' (n 4) 77 at 92); Halaburda, 'Blockchain Revolution without the Blockchain' (n 46).

[59] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 26.

[60] Eric Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts', *Tilburg Private Law Working Paper Series* 6 (2017) 2.

[61] Scott Farrel, Heide Machin, and Roslyn Hinchliffe, 'Lost and Found in Smart Contract Translation – Considerations in Transitioning in Legal Architecture', *J.I.B.L.R.* 33(1) (2018) 24.

[62] For Lin William Cong and Zhiguo He, smart contracts are not 'entailing artificial intelligence (on the contrary they are rather robotic)', Cong and He, 'Blockchain Disruption and Smart Contracts' (n 29) 8.

[63] Finck, 'Blockchains: Regulating the Unknown' (n. 1) 665 at 670; Werbach and Cornell, 'Contracts Ex Machina' (n 55) 313-381; Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 24-25; Kõlvart, Poola and Rull, 'Smart contracts' (n 11) 135.

event-driven insurance'[64], 'automatic compensation due to flights delay, car leasing contract,[65] tax compliance,[66] freight and logistics industry,[67] not to mention the most cited of vending machines.[68] In these law fields, smart contracts are seen as an efficient 'consumer rights enforcement'.[69] Hence, Blockchain technology can be suitable 'to track movement of goods and payments', within international commerce,[70] smart energy grids,[71] micropayments related to 'ecosystems of peer-to-peer transactions', collaborative platforms, and so on.[72]

The common feature in all those examples is the clause simplicity of the contracts. And the advantages of the technology above-mentioned are identifiable in this field: the lower

[64] Stan Higgins, 'AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product' (coindesk, 13 September 2017). Retrieved 4 March 2019 https://www.coindesk.com/axa-usingethereums-blockchain-new-flight-insurance-product/.

[65] This is the example given by Hanna Halaburda: 'upon a missed payment, the car would automatically lock, and control would return to the lender' (Halaburda, 'Blockchain Revolution without the Blockchain' (n 46) 5).

[66] Although the experience has been the 'first iteration of the employment tax use case, and therefore addressed only part of governments' complex tax requirements', the US experience was based on the idea of cost reduction ('Code as Law: Using Ethereum Smart Contracts to Ensure Compliance with Federal Tax Law'. Retrieved 4 March 2019. https://media.consensys.net/code-as-law-using-ethereum-smart-contracts-to-ensure-compliance-with-federal-tax-law-3fc67cb7b956.

[67] Cong and He, 'Blockchain Disruption and Smart Contracts' (n 29) 17.

[68] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 5.

For the use of smart contracts in corporate finance and governance, see David Yermack, 'Corporate Governance and Blockchains', *Review of Finance* (2017) 7 at 26.

[69] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 5. As the author states, the German government has 'set out to evaluate smart contracts in relation to consumer contracts'.

Martin Fries, 'Law and Autonomous Systems Series: Smart consumer contracts – The end of civil procedure?'. Retrieved 4 March 2019 https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/smart-consumer-contracts-end-civil-procedure.

[70] Some law firms, regarding international contracts, are working in digital terms related to insurance, 'outlining key terms … and modelled an Ethereum-based smart contract based on this term sheet to govern relevant payouts'. The experience allowed the comparison between smart contract and natural language one and the identifications of some legal vulnerabilities [Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 77-78]. The example is from Steven Norton, 'Law Firm Hogan Lovells Learns to Grapple with Blockchain Contracts', *The Wall Street Journal*, 1 February 2017). Retrieved 9 March 2019 https://blogs.wsj.com/cio/2017/02/01/law-firm-hogan-lovells-learns-to-grapple-with-blockchain-contracts/.

For a more detailed overview of this issue, *see*, for instance, Harry Surden, 'Computable Contracts' *UC Davis Law Review* 46 (629) (2012). Available at https://ssrn.com/abstract=2216866.

[71] About Blockchain and its use in the energy sector, with some examples, Dentons, 'Blockchain in the Energy Sector: Evolving Business Models and Law', *International Energy Law Review* 7 (2018) 233-269.

[72] Finck, 'Blockchains: Regulating the Unknown' (n 1) 665 at 671 ff.

transactions costs and the reduction of 'counterparty risk and interpretative uncertainty'.[73] Therefore, smart contracts are expected to be the end of court disputes and the guarantee of full transparency in both contract conclusion and execution.[74] Even though their effects, as Michèle Finck stresses, can be altered by another smart contract.[75] They are presented as an alternative to traditional contracts.[76]/[77]

But the disadvantages of Blockchain technology identified above are mirrored in smart contracts, namely regarding security.[78] The contract code can have bugs, the access key can be broken, and user behaviour can endanger its security. In March 2015, the Ethereum Foundation commissioned a security report[79] from Least Authority about the Ethereum Virtual Machine containing best-practice recommendations.[80]

This technology is being pointed out as adequate for contract execution.

[73] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 25. Primavera di Filippi and Aaron Wright also point out that this feature also favours 'new avenues for commercial relationships, potentially facilitating an increasing range of economic activities between untrusting parties' (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 81).

[74] This advantage can be misleading as the smart contract does not enshrine the guarantee of no dispute at all. That is why it has been discussed how 'arbitration mechanisms' could be included in sophisticated smart contracts. See Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 27; Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 25.

[75] Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 25.

[76] Addressing several relevant issues concerning contract formation such as capacity, contracting under mistake, the moment of agreement, connection between related contracts, certainty of terms, remedies and interpretation, Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective, *Computer Law & Security Report* (n 3) 1 at 6 ff.

[77] Primavera di Filippi and Aaron Wright address the possibility of replacement from a privacy issue point of view: the 'privacy issues may limit the potential for smart contracts to replace traditional legal contracts in many commercial settings. Without strong privacy protections, smart contracts likely will prove unsuitable for legal agreements where confidentiality is crucial', (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 83). Referring to this concern, Brydon Wang Allens, 'Blockchain and the law' *Internet Law Bulletin* 19 (1) (2016), 250-254.

[78] Addressing security issues in smart contracts, Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (n 2) 490 at 517.

[79] Retrieved https://github.com/LeastAuthority/ethereum-analyses/blob/master/GasEcon.md#callstack-depth-limit-errors.

[80] Zikai Alex Wen and Andrew Miller state that most of those recommendations were ignored ('Scanning Live Ethereum Contracts for the 'Unchecked-Send' Bug', retrieved http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/.

The contractual obligations are translated into programming language or ‘contractware’.[81] One of the advantages of computer language, when compared to the traditional one, is less ambiguity, ‘because there are simply fewer terms that a computer can recognise than a human can’.[82]

Although it may seem a new, ‘perfect’ way of contracting, the smart contract execution method raises several legal questions.

First, the feature of language simplicity and accuracy only applies to very basic contracts, mainly those which entail simple obligations and are plain executions of law basics.[83] And it is imperative, in each smart contract, to assess if the contractual provisions in a code are valid and effective under law.[84]

The inherent immutability regarding code language does not allow the contract to keep up with changing circumstances; the occurrence of partial breach of contract by one of the parties; and the consideration of non-compliance due to third-party involvement. In other words, if the programming language equals ‘if/then’ clauses, how are particular circumstances that do not meet the if-clause to be considered? A computer cannot recognise imperfect performance unless all the possible conditions are turned into computer language and the consequences are set out as well.[85] Therefore, the described

[81] That is, ‘physical or digital instantiations of contract terms onto machines or other property involved in the performance of the contract’, Raskin, ‘The Law and Legality of Smart Contracts’ (n 54) 305 at 307.

[82] Predictability and unambiguity are the features that allow the execution of smart contracts without performance problems (in this sense, Farrel, Machin and Hinchliffe, ‘Lost and Found in Smart Contract Translation – Considerations in Transitioning in Legal Architecture’ (n 61) 25). Identifying the ‘inherent’ flexibility and ambiguity of natural language of law, Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 199.

[83] Being a technology, code language can become more and more complex and it can evolve and embrace more sophisticated clauses.

[84] Farrel, Machin and Hinchliffe, ‘Lost and Found in Smart Contract Translation – Considerations in Transitioning in Legal Architecture’ (n 61) 24 at 25.

[85] Primavera De Filippi and Aaron Wright acknowledge these types of problems (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) *200*). Recognising these concerns, Sope Williams-Elegbe, ‘Public Procurement, Corruption and Blockchain Technology: A Preliminary (Legal) Inquiry’. 2018. Inaugural lecture delivered on 25 October 2018. Retrieved 5 December 2018 https://www.sun.ac.za/english/Documents/newsclips/InauguralLecture_ProfSopeWilliamsElegbe_23Oct2018.pdf.

immutability in smart contracts should be seen as a disadvantage per se, related to the difficulty in translating legal clauses into code. This difficulty, in my belief, should not be confused with the recognised (and needed) existence of some uncertainty regarding the definition of legal contracts,[86] and that can explain other ways of legal binding such as Heads of Agreements, Memorandums of Understanding, Letters of Comfort, Side Letters and Letters of Intent.[87] Furthermore, it should not be confused with non-concluded contracts: a contract can be concluded if the parties have already agreed upon the essential obligations, but they are not obliged to agree upon every other obligation. They can also agree to agree later on upon eventual circumstances that may or may not arise.[88]/[89]

The need to accommodate future changes in public contracts is recognised upfront by the legislator, foreseeing discretionary clauses or concepts. These provisions imply an exercise of reason, discretionary powers or a judgement of foresight, and making the if-clause inadequate and useless.[90] In fact, most contracts are far more complex than the simple if/then rule.[91] Yet, it should also be pointed out that it is very oversimplified to

[86] Depending on the legal order (either Anglo-Saxon law or continental law), some contracts rely upon legal provision to solve any unforeseen regulation in the contract such as abnormal and/or unpredictable change of circumstances. This kind of unforeseen regulation relies, for instance, in continental law, upon the civil code's provision.

[87] Ralph B. Lake and Ugo Draeta, *Letters of Intent and Other Precontractual Documents*. 2nd Edition. (New Hampshire, 1994).

[88] Of course, always within the legal contractual autonomy. Even in public contracts, the 2014 Directives foresee the possibility that in contract execution there can be contract modifications in several situations. One of them is when that possibility is previously foreseen in public procurement procedure documents.

[89] Addressing the transaction costs within the so-called 'incomplete contracts', Jean Tirole, 'Cognition and Incomplete Contracts', *American Economic Review* 99(1) (2009) 265-294. http://www.aeaweb.org/articles.php?doi=10.1257/aer.99.1.265.I. Idem, 'Incomplete Contracts: Where Do We Stand?', *Econometrica* 67(4) (1999) 741-781. Retrieved http://www.jstor.org/stable/2999457. Nevertheless, the incompletion of a contract cannot mean the hiding of essential elements from the other contractual partner or the misleading about its features. In these cases, there can be a lack of agreement upon the essentials of the contract or the contract may be void. Of course, there are costs in foreseeing all the future needs of the contractual relationship. At least in continental law, usually the civil code has provisions to solve this kind of situations.

[90] Farrel, Machin and Hinchliffe, 'Lost and Found in Smart Contract Translation – Considerations in Transitioning in Legal Architecture' (n 61) 24 at 25.

[91] Max Raskin, in a simple analysis, states: 'the enforcement of a contract is nothing more than the running of a circumstance through a conditional statement'. Therefore, a machine is able to enforce a simple contract and with cost reduction (Raskin, 'The Law and Legality of Smart Contracts' (n 54) 305 at 315). This is the case provided that there is no judicial discretion grounded in legal discretion.

assume that software code can only go so far as the if-then clauses. Nowadays, even before AI solutions, code programmers can already translate into software very complex syllogisms with several alternative conclusions. However, our main critical point relates to concept interpretation, whenever it is needed. There are legal concepts such as good faith, necessary measures or even proportional outcomes that cannot be translated into code language (only into if-then clauses using the concept in its natural language) but are fundamental to contract execution and can only be determined, in each situation, by interpretation and reasoning.[92] These concepts are crucial to allow parts not to make the useless effort to foresee all scenarios in contract execution. There are too many costs and ultimately, it is an impossible mission.

Thus, the removal of language ambiguity – which, within administrative law ambiguity, reappoints to discretionary legal language, which enables the best singular decision by administrative bodies, therefore fulfilling the best public interest pursuit – has disadvantages regarding the permanent possibility of adapting the contract to the environmental context.[93] Eric Tjong Tjin Tai suggests a set of steps in constructing a smart contract, while recognising up front a set of difficulties, such as the two mentioned above, and adding the need for 'balancing the relative interests of parties', which, in the future, can be overcome by Artificial Intelligence. For now, smart contracts are very simple ones. But, as Merit Kõlvart, Margus Poola, and Addi Rull state 'if a computer program must take care of all the main contractual steps, including pre-contractual negotiations, formation and performance of the contract, dispute resolution, and take into

[92] In this sense, Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 6; Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 27.

[93] Primavera Di Filippi and Aaron Wright recognise that this ambuiguity 'provides flexibility to parties while also cutting down the time and expense of negotiation. In many cases, vagueness may in fact result in more efficient contracts' (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 77). Regarding this issue in commercial/private law, George G. Triantis, 'The Efficiency of Vague Contract Terms', *Louisiana Law Review* 62(4) (2002) 1065-1079. Available at https://digitalcommons.law.lsu.edu/lalrev/vol62/iss4/4.

account laws applicable to a particular transaction, then it requires the capability of a very advanced artificial intelligence.'[94]

Secondly, the code language must be confronted with the no-turning back execution feature whenever the transaction is made. Particularly, as Michèle Finck stresses, if it is unwanted. The other drawbacks have already been pointed out, namely contract execution by whom is lacking legal capacity, the issues regarding the default, and the legal implementation of contract modifications ordered by court.[95]

This being said, one must also point out that there is no unanimity regarding the total inadequacy of smart contracts related to extraordinary execution or out of estimation clauses. In fact, Michèle Finck herself recognises the oracle solution. And other authors, like Primavera Di Filippi and Aaron Wright, when addressing that solution, also point out its adequacy to 'interact with real-world persons and potentially react to external events'.[96] The legal concept of 'change of circumstances' can be included in this potential reaction. For Primavera Di Filippi and Aaron Wright, the contract parties 'can refer to an oracle to modify payment flows or alter encoded rights and obligations according to newly received information'.[97] It is true that, in this case, the 'oracle' should be a human because only humans can make evaluations, weighing factors according to legal criteria.[98]

[94] Kõlvart, Poola and Rull, 'Smart contracts' (n 11) 135.
[95] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 5.
[96] Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 75.
[97] *Ibid* 75.
[98] Considering this dimension, although in general contracts and not public contracts (where there are multiple legal constrains), Di Filippi and Wright, *ibid* 75.

Whenever the contractual relationship is further complex, Primavera Di Filippi and Aaron Wright propose the hybrid agreements, which can be proven useful whenever 'open-ended terms that outline performance obligations' are set out.[99]

Another way of proceeding is the 'sophisticated smart contract' that Michèle Finck acknowledges. This solution is thought to cover more complex circumstances and foresees human intervention with the use of 'multiple-signature verification ('MultiSign') whereby the parties need to activate the software with their respective private keys before it can execute'.[100] In such cases, there is human intervention and therefore the issues regarding Article 22 GDPR are avoided.[101]

Hence, some solutions are presented, such as outside agreements on overriding rules and reliance on third-party input.[102] But there are some other legal boundaries between contractual parties that can be difficult to comply with, such as interaction and communication, as it is very complex to translate such kind of obligations into programming language. As the author recognises, the smart contract is fit to 'allow parties to deduce how they should act in certain situations', but it is unfit to solve discretionary situations, including temporal issues.[103] In fact, as Max Raskin acknowledges, 'automation ensures performance, for better or worse, by excising human discretion from contract execution'.[104] Therefore, 'users of smart contracts will have then to accept the limitations of smart contracts in providing everything that contract law can provide regarding the protection of party interests'.[105]

[99] *Ibid* 77. See above the distinction between incompletion and immutability or inadequacy to be translated into software code.

[100] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 25; Finck, *Blockchain, Regulation and Governance in Europe* (n 4) 27. Explaining the Multisig, Werbach, *The Blockchain and the New Architecture of Trust* (n 6) 109 ff.

[101] See *infra*.

[102] Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts' (n 60) 1 at 4.

[103] Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts' (n 60) 1 at 7.

[104] Raskin, 'The Law and Legality of Smart Contracts' (n 54) 305 at 306.

[105] Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts' (n 60) 1 at 8.

Finally, the main questions regarding enforcement, breach and remedies, which, most of the times, imply third-party intervention, are not solved.[106] Although, regarding simple contracts, the oracle solution[107] can be applied. Kevin Werbach gives the following example: a ‘simple smart contract in which each of the parties has a private key and a third key is given to an expert arbitrator. The smart contract requires two of three keys in order to execute. If the parties agree the contract has been fully performed, they each provide their key and the smart contract executes. If there is a dispute, they turn to the arbitrator. She either provides her key along with that of the party seeking to enforce the contract or refuses it and therefore prevents completion of the transaction. This system mimics a legal arbitration process.’[108] But even for some authors, this option does not remove the possibility of ultimate Court ruling.[109]

All of the disadvantages considered made Michèle Finck doubt whether smart contracts are real contracts and smart. In fact, the if-then clauses exclude ‘wider contextual factors’, and they need ‘oracles’ to feed the system in order for the if-then clauses to be verified.[110] Therefore, the author adheres to a different concept proposed by Ari Juels, Ahmed Kosba and Elaine Shi, namely ‘an autonomously executing piece of code whose inputs and outputs can include money’.[111] But these features also allow the conclusion that ‘in essence, smart contracts are mechanisms designed to achieve the automated execution of

[106] Primavera di Filippi and Aaron Wright recognise that ‘Courts ultimately retain jurisdiction over legal effects of a smart contract’ (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 78).

[107] Oracles are external sources, either human or automated data, which feed the smart contract. This feature explains why Primavera De Filippi and Aaron Wright sustain that smart contracts are ‘more dynamic than traditional paper-based contracts, because they can be constructed to adjust performance obligations’ (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 75).

[108] Werbach, ‘Trust, but Verify: Why the Blockchain Needs the Law’ (n 2) 490 at 548.

[109] Particularly in the United States. See Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 79.

[110] Finck, ‘Blockchain and Data Protection in the European Union’ (n 18) 1 at 4.

[111] Ari Juels, Ahmed Kosba and Elaine Shi, ‘The Ring of Gyges: Using Smart Contracts for Crime’. Retrieved 4 March 2019 http://www.arijuels.com/wp-content/uploads/2013/09/ Gyges.pdf. Finck, ‘Blockchain and Data Protection in the European Union’ (n 18) 1 at 4.

software code. This makes them a method to *automated* data processing'.[112] If so, as it seems, they are in a collision course with the qualified prohibition of 'solely automated data processing' in the GDPR.[113] Therefore, if smart contracts fall under the definition of 'solely automated data processing', the compliance with GDPR imperative provisions must be addressed. In fact, they display the two features referred by Michèle Finck: (i) they count as 'a decision based solely on automated processing'; and (ii) that decision 'produces legal effects for the data subject'.[114] The A29WP guidance establishes that solely automated decision-making is 'the ability to make decisions by technological means without human involvement'.[115] In order to consider smart contracts to be under the Article 22 (1), Michèle Finck proposes two 'alternative interpretations': 'the 'decision' could be considered to simply be the execution of the smart contract code upon occurrence of a pre-determined event such as a decision whether a given fact justifies payment or reimbursement of a given sum. In line with the very rationale of smart contracts, there is no human involvement at the stage of 'the decision', meaning that Article 22(1) applies to such software'; the other ''decision' encompasses a broader timescale' and 'in many circumstances, humans will be agreeing on the purpose and set-up of the smart contract. Sometimes, a human will act as the oracle feeding the smart contract input data needed to execute'.[116]

[112] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 6.
[113] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 6. See article 22 (1).
[114] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 6.
[115] A29WP, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (wp251rev.01), 8. Retrieved 4 March 2019 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
Merit Kõlvart, Margus Poola, and Addi Rull expressly refer that 'a smart contract is an intelligent agent. In other words, it is a computer program capable of making decisions when certain preconditions are met'. (Kõlvart, Poola and Rull, 'Smart contracts' (n 11) 134).
[116] Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 7-8; 9. 'If human involvement in the elaboration of the contract were to be taken into account for the purposes of the first paragraph, there would be no need for an explicit exemption to this effect in the second paragraph.

3. Mandatory e-procurement and some neighbouring issues

Some of the advantages and disadvantages of Blockchain technology can be found in a neighbouring subject much related to public procurement: e-procurement and the dematerialization of public procurement procedure[117].

Although its mandatory feature was only set out in 2014 Directives, e-procurement has been a goal in EU law. The *Green Paper on expanding the use of e-Procurement in the EU SEC (2010) 1214* defined e-procurement as 'the use of electronic communications and transaction processing by government institutions and other public sector organizations when buying supplies and services or tendering public works'[118]. An electronic procedure within public procurement means much more than the dematerialization of the procedure. It includes the legal provision of new phases such as electronic auctions (e-auctions) and dynamic purchasing systems. Digital tools are considered by EU law as 'more transparent, evidence-oriented, optimised, streamlined and integrated with market conditions'.[119]

Concerning the procedure itself, besides the downsizing of administrative costs, transparency and efficiency, the electronic procedure also annuls the need for repeated documentation submission. As it can be read in some other EU Commission papers regarding this issue, the electronic procedure implies the 'replacement of paper-based

[117] For further details regarding the implementation of e-procurment in Portugal, Raquel Carvalho, 'Directive 2014/24/EU and Implementation of e-Procurement in Portugal', European Procurement & Public Private Partnership 1 (2019), 43.

[118] Commission, Green Paper on expanding the use of e-procurement in the EU (SEC (2010) 1214 final, 2010).

[119] Commission, E-procurement, retrieved https://ec.europa.eu/growth/single-market/public-procurement/e-procurement_en.

procedures by ICT-based communications and processing throughout the procurement chain. E-Procurement involves the introduction of electronic processes to support the distinct phases of a procurement process – publication of tender notices, provision of tender documents, submission of tenders, evaluation, award, ordering, invoicing and payment'.[120]

Currently, though, some critical neighbouring issues have been highlighted in e-procurement. Despite huge gains in administrative costs (economic efficiency), issues have arisen concerning data integrity and protection from the point of view of both economic operators and contract authorities when using electronic platforms. Furthermore, there are some concerns regarding the system information integration, the authentication and identification of the tenderers, interoperability between platforms that gather information, and the costs to access them, because these electronic platforms are a centralised technology.[121]

One of the key issues when using electronic platforms is the need to own several timestamps to be able to access different electronic platforms, as it implies a burden and cost to economic operators and tenderers. This is one of the reasons why the Portuguese law that has transposed article 22 stresses the importance of interoperability, stating in article 36 that 'management companies must comply with the necessary interconnection and interoperability among themselves, so that economic operators can choose the electronic platform freely, regardless of the one used by the contracting authority'.
Certificated chain validation is assured by law through electronic, certified mandatory signatures.[122]

[120] Commission, Communication on 'End-to-end e-procurement to modernise public administration', 2013.
[121] The dematerialisation costs are related to timestamps access, but it has been tried to gradually reduce them.
[122] See article 54 of Law 96/2015.

Another difficulty has been the upload of tenders and documents, due to technical issues. This may be one of the contact points with Blockchain technology, as it already displays some of the information contained in those documents, only remaining the interoperability and data protection issues.

Last, but not least, electronic platforms raise data protection issues regarding the security and accuracy of both personal data and commercial and industrial secrets. Articles 39 ff. of the above-mentioned law provide for the legal regulation concerning these matters and establish some duties for the electronic platform's responsible party.

Data integrity is seen as a key feature to assure transparency in e-procurement procedures. In Portuguese law, these concerns are solved by means of individual accounts and authentication, access codes, and the use of timestamps and document encryption. Given the importance of the tender and the documents that support it, electronic platforms must have archive systems fully accessible within the procedure duration, but only to those involved in the procedure, ensuring the secrecy of the proposals within the time to present them, which means the need to implement security procedures regarding access and cyber-attacks. And after this period of bidding, the proposals and supporting documents must remain unchangeable throughout the legal period of maintenance. Yet, these documents are only available for this procedure. When another public procurement is launched, another electronic procedure begins, along with the same problems and the same need to upload documents already uploaded in other procedures…

4. Is Blockchain technology fit for public procurement procedure?

Public procurement is known to be a procedure which embodies transparency, integrity and efficiency, but also to be a competitive and risk-averse procedure.

4.1. Moments with sensitive issues

Public procurement procedures require tender submission within a preestablished period of time and usually, as we have seen, its upload in an electronic platform (at least in public procurement procedures above thresholds). Depending on the contract subject, some 'private' data, concerning industrial, commercial or intellectual property, can be involved in the proposal.[123] The solutions enshrined herein contain the tenderer's advantage in the procedure and are therefore most of the times protected by law (patent law, for instance). Simultaneously, the information must remain anonymous and be identifiable only for a few people. Then, after the tender submission deadline, normally, all tenderers want to access every other tenderer's proposal and, after the evaluation period, the jury's assessment. This limited transparency fulfils the general goal of transparency and helps to build trust among tenderers.

Therefore, Deividas Soloveicik identifies two moments when confidentiality is a key issue within public procurement procedure: (i) when the tenderers want to access information on other tenderers' or bids; and (ii) when the tenderers want to access information related to the evaluation of one's bid.[124] The 2014 Public Procurement Directives had already addressed this issue.[125] Article 21 expressly sets out 'technical and trade secrets' and 'confidential aspects of tenderers' concerning other bids, not disregarding internal law protections. On the other hand, article 55 (3) provides that

[123] For an analysis of copyright law and blockchain, Finck and Moscon, 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0' (n 4) 77 at 108.

[124] 'Rethinking the confidentiality in public procurement: does *public* mean *naked public*?', Reprint from *Procurement Law Journal* 1 (2018) 11 at 11.

[125] Articles 21 (1) and 55 (3) of the 2014/24/EU Directive.

‘contracting authorities may decide to withhold certain information (…) regarding the contract award (…) where the release of such information would impede law enforcement or would otherwise be contrary to the public interest, would prejudice the legitimate commercial interests of a particular economic operator, whether public or private, or might prejudice fair competition between economic operators’.[126] This last provision has to abide by the general guidance of the obligation to provide the reasoning and grounds behind the public procurement decisions.[127]

After the award, the successful tenderer must give evidence of the inexistence of exclusion grounds. Article 57 of the 2014/24/EU Directive establishes a set of reasons that, when present, and regarding the successful tenderer, determine that another tenderer must be chosen. Some of them can be overcome by the so-called self-cleaning procedure; others by documental proof of inexistence. In fact, the Directive establishes that ‘any economic operator that is in one of the situations referred to in paragraphs 1 and 4 may provide evidence to the effect that measures taken by the economic operator are sufficient to demonstrate its reliability despite the existence of a relevant ground for exclusion. If such evidence is considered enough, the economic operator concerned shall not be excluded from the procurement procedure’. In what concerns the exclusion grounds that may be overcome by documental proof – breach of obligations relating to the payment of taxes or social security contributions – those can be archived in electronic, public, platforms. But regarding, for instance, fiscal situations, this circumstance is included at

[126] There also some case law where the CJEU has analysed this issue: Case C-450/06, *Varec*, ECLI:EU:C:2008:91; C-629/11. *Europaïk Dynamiki v. Commission* (ESP-ISEP), ELI:EU:C:2012:617; Joined Cases T-339/10 and T-532/10, *Cosepuri v. EFSA* (EFSA), ECLI:EU:T:2013:38.

[127] Soloveicik, ‘Rethinking the confidentiality in public procurement: does *public* mean *naked public*?’(n 123) 11 at 23.

Being critical about the ‘excessive transparency’ in public procurement, Albert Sanchez Graells, ‘The difficult balance between transparency and competition in public procurement: some recent trends in the case law of European Courts and a look at the new Directives’, *University of Leicester School of Law Research Paper* No. 13 – 11, 2013, https://ssrn.com/abstract=2353005.

least in the concept of confidential information and, therefore, benefits from both constitutional and legal protection.

Therefore, this is a sensitive issue for the law regarding both data protection and public procurement rules. At some point of public procurement procedure, some personal data and private data are required. The former mostly regarding solvency, fiscal and social security compliance; the latter, commercial or/and industrial property that substantiate every tenderer's advantage.

The innovation feature regarding the use of electronic platforms has raised quite a few critical issues that are precisely connected to those requirements. So, naturally, the main question that comes to mind is whether there is room for Blockchain as a solution for granting transparency and the necessary accuracy and truthfulness of data, overcoming the key issues regarding the 'traditional' use of electronic platforms in public procurement procedure.[128]

The latest Directives show a deep concern regarding this trilogy: there are numerous provisions respecting announcements and information disclosure; new dispositions concerning conflicts of interests and exclusion grounds; and some provisions are aimed to achieve more efficiency by making, for instance, e-procurement mandatory.

Although innovation is one of the pillars of the latest Directives, and such a system is undoubtedly innovative, one must not forget that the search for the 'best value for money' must be accompanied by some guarantees, mainly within two important moments of the public procurement proceeding: when economic operators present their proposals, and when they must prove their integrity, demonstrating that there are no grounds for

[128] Concerning public contract execution, that is a somewhat different question.

exclusion. The former usually includes sensitive information regarding the commercial or industrial status, while the latter relates to personal and sensitive information which is legally protected as fundamental rights under both the General Data Protection Regulation (GDPR) and constitutional law and sometimes relies on confidentiality. Hence, is there irreconcilability between this qualification and both the permission of broad access to it and the 'impossibility' of its withdrawal from that kind of system?

4.2. Comparing technological solutions within the drawbacks and difficulties identified

This being the framework, can Blockchain technology be useful in overcoming the shortness of actual e-procurement solutions? Is it a better and more suitable choice than traditional electronic platforms?

According to Roland Berger, there are some prerequisites that have to be fulfilled to define 'a meaningful use case of blockchain': i) Do you need a shared database?, ii) Do you need read and write access for multiple users?, iii) Do users mistrust each other?, and iv) Do you want to avoid an intermediary?[129] If we pose these questions to a contracting authority within public procurement procedure, the answer to all the questions will be most probably positive:

(i) yes, in public procurement, a database is needed because there is information regarding the tenders and/or candidates;

(ii) the information within must be read not only by the contracting authority (and the internal bodies that will assess the tenders) but also by all the economic operators when the period of maintenance of proposals is finished. The importance and the role of the

[129] Berger, 'Blockchain – A Promising Technology for the Belgian Public Administration' (n 2).

access can be slightly different: contracting authorities must access to verify the fulfilment of legal requirements and to evaluate; the candidates/economic operators, to fulfil a democratic role, regarding transparency;

(iii) although at first, all the economic operators need to access and upload documents, after the tender presentation period is finished, it is crucial that the accuracy of the information supporting the tender is untampered so that the comparison among all tenders is as equal and transparent as possible;

(iv) this immutability alongside other 'immutabilities' such as those of the criteria and evaluation factors and the absence of intermediaries (important to diminish the risk of tampering[130]) grants that each tender stays as it was uploaded, sustaining trust and decision-making transparency among economic operators in public procurement. Although interested in a transparent procedure, all economic operators in public procurement remain as competitors.

If the public administration cannot answer all questions affirmatively, and the question regarding mistrust cannot be answered, then only a shared data-base is needed.[131]

As for data storage, can Blockchain provide a better solution? Normally, the public-produced information such as fiscal and social security compliance and criminal records is stored in databases, not accessible to all, precisely due to the private or protected feature of the data. But as Primavera Di Filippi and Aaron Wright stress, 'like all fortresses, however, even the most secure data centres have vulnerabilities. (…) Blockchains are viewed as a new tool to build more reliable and transparent government registers and

[130] Tamper-resistance is one of the attractive key features.

[131] Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 6. Nevertheless, public procurement rules impose a lot of guarantees that favour trust: the broad publicity of the competition and the procurement documents, the notification of the choice, the grants that the contracting authority has to provide to conclude the contract, and so on.

record-keeping systems to modernise and increase secure critical information'.[132] This is a different dimension of Blockchain usage: not for public procurement itself but for the present database-stored information. As data integrity is a much-needed asset in public procurement, Blockchain technology can offer it, provided that the data uploaded is accurate in itself. This guarantee, however, is given outside the Blockchain technology, as the uploaded of information is carried out by public authorities. Therefore, whenever inner accuracy is non-arguable, immutability and traceability are the features that can assure that integrity.[133] As Jason Killmeyer, Mark White, and Bruce Chew stress, 'a blockchain database retains the complete and indelible history of all transactions, assets, and instructions executed since the first one'.[134] Therefore, it is possible, at any moment, to reconstruct all the data inserted and the respective date.

Hence, an option as such could be very interesting for public procurement procedures if the interoperability issues and data protection issues were to be guarded against.

It is also unarguable that a Blockchain system acknowledged by different entities at its various stages provides a prominent level of transparency, because validation is not carried out by one single entity.[135]

However, in public procurement, the principle of transparency is not the primary regulation. It must be adjusted and harmonised with the competition principle, which

[132] Killmeyer, White and Chew, 'Will Blockchain Transform the Public Sector? Blockchain Basics for Government' (n 2). These remarks can also be made or be useful regarding the register of property assets or commercial/industrial inventions.

[133] Concerning traceability, every transaction is signed and timestamped.

[134] Killmeyer, White and Chew, 'Will Blockchain Transform the Public Sector? Blockchain Basics for Government' (n 2).

[135] However, as Lin William Cong and Zhiguo He say, 'empirical evidence suggests that greater information sharing indeed facilitates collusion' Cong and He, 'Blockchain Disruption and Smart Contracts' (n 29) 27. About collusion in Blockchain and Smart contracts, see Thibault Schrepel, 'Collusion by Blockchain and Smart Contracts' *Harvard Journal of Law and Technology* 33. 14 January 2019. Available at https://ssrn.com/abstract=3315182 (http://dx.doi.org/10.2139/ssrn.3315182).

sometimes collides with transparency, and this feature has important consequences to the Blockchain governance. In fact, during public procurement procedure, there are stages with broad publicity, followed by other with restrictive solutions, and broad publicity again at the end. So, a unique Blockchain solution could never be suitable.

We are currently at a sensitive crossroad. If we use a Blockchain system, data are verified and therefore accessible and guaranteed as they are uploaded. Yet, legal systems protect and reserve that information at a prominent level, namely at a constitutional level. Who, then, decides what information is verified in the Blockchain? Who is accountable for that decision? Who authenticates the data uploaded? Is there an obligation to feed that kind of system? Will it be mandatory to allow personal or business information to be kept in that kind of system to be able to participate in public procurement proceedings? If the data provider can be, to a certain level, the data controller, is this solution suitable for all kinds of personal data? Are there technical remedies for these concerns within the Blockchain system?

Let us address and test sensitive data within public procurement procedure. Would the existence of a Blockchain containing the sensitive information regarding exclusion grounds be possible? The public procurement procedure running on an electronic platform could be interoperable with a Blockchain solution if and when the contracting authority needed to consult that kind of information.[136] The data would be more reliable. For such a scenario, in terms of governance, what could be the most suitable solution: a public/permissionless blockchain accessible through private keys, with encrypted information and the information owner as the sole responsible for the accuracy of data;[137]

[136] As we have already seen, the oracle solution can be applied to this situation. Whenever public records, while containing sensitive or even personal data, could be functioning as an oracle to the procurement procedure, this is a viable way to proceed.

[137] The solution presented like this is a very simplified description as some relevant personal information, in order to be trustworthy, has to be produced by public authorities such as Fiscal Administration or Social

or a private one, with a gatekeeper and limited access? Access would be temporary – only for each procedure and within procedure rules – and the cost of uploading documents would be considerably decreased.

The interoperability solution could probably solve some of the risks that are nowadays a concern in centralised electronic procurement: traceability; immutability of data; accuracy and transparency.[138]

Concerning immutability, although being an interesting feature when considering information trust, it could also pose a disturbing question: how would it be possible to redraw a proposal if a tenderer changed his mind, or replace the uploaded proposal for another before the deadline for submission? This immutability feature is very useful during the maintenance period of the proposals, fulfilling the Directive's goal regarding equal competition. But it is not always a desirable feature in all the stages of public procurement procedure.

One can consider using Blockchain to implement a public procurement procedure, i.e., to conclude a contract. The procedure rules would need to be translated into code, from the rules to present proposals, including the proposal evaluation formula with criteria award, to the rules to exclude proposals and tenders, the habilitation rules and, the best tender having been chosen, the rules of contract execution.

This option would benefit from Blockchain's transparency and immutability features. The tenderer, with his key, consults the rules, develops his tender and then uploads it, fulfilling

Services or even by a Government Department (for instance, regarding criminal records). Although the data is personal, its trustworthiness and accuracy need to be verified and attested to a different person.

[138] Joseph Huntington La Cascia, reflecting upon the use of Blockchain in public procurement in the context of World Bank business, sustains that this technology is particularly fit to e-procurement systems as 'every procurement transaction is on a ledger'. And 'blockchain can streamline the process by integrating with other systems more easily through smart contracts' (Joseph Huntington La Cascia, 'Blockchain Lessons for Procurement'. Retrieved 5 December 2018 https://wbnpf.procurmentinet.org/featured/blockchain-lessons-procurment.)

all the security requirements, such as the signature key. As the deadline to upload the tenders is enshrined in the code, when it has passed, the Blockchain no longer allows the upload of more tenders. Then the tender evaluation begins, which can also be made by the Blockchain technology, applying the evaluation formula. This option grants a much more unbiased outcome. From this point on, tenders' graduation is uploaded to the Blockchain and the consultation period is open to all tenderers. Afterwards, depending on the legal regulation of public contracts, the chosen tenderer must prove his/her personal integrity, comply with other formal and substantial requirements and conclude the contract to be executed.[139]

This Blockchain solution would also allow citizens to consult not only the tenders and the evaluation formula (and its outcome), but also the concluded contract, as a transparency and democratic control measure, becoming an instrument to fight corruption in public procurement procedures.[140] Corruption has become a major problem in some countries, and the European legislator has established some provisions concerning this problem. However, whenever discretionary powers are provided for in the evaluation stage of public procedures, there is the inherent risk of human intervention. The use of technology in the assessment will naturally decrease the likelihood of bias.

This option would imply a complex programming system and it is very likely that, for each public procedure, a specific Blockchain would be created. Each public procurement

[139] Analysing a similar procedure, Freya Sheer Hardwick, Raja Naeem Akram, and Konstantinos Markantonakis, 'Fair and Transparent Blockchain based Tendering Framework – A Step towards Open Governance'. 2018. arXiv:1805.05844v1 [cs.CR] 15 May 2018 (DOI: 10.1109/TrustCom/BigDataSE.2018.00185), 1.

[140] Referring to the 'futility of traditional legal responses to procurement corruption', Sope Williams-Elegbe has shifted her research in this subject to the Blockchain solution and its use in public procurement procedure (Sope Williams-Elegbe, 'Public Procurement, Corruption and Blockchain Technology: A Preliminary (Legal) Inquiry' (n 85)).

procedure has its specific features concerning contractual provisions from the contracting authority.

As we have already seen above, technology cannot yet address complex demands of public buyers, as their needs are related to public interest and therefore difficult to be put into mandatory, non-discretionary provisions only. Discretion is a legal instrument necessary to allow public officials to make the best administrative decision within the law and the bounding pursuit of public interest. Put differently, the mere disappearance of administrative discretionary powers is not the solution. Blockchain can be added to the existing measures, benefitting from the interoperability with some databases or oracles (whether human or electronic platforms), but for now it has some other drawbacks, for instance, how to apply legal safeguards concerning personal data, commercial and industrial secrets guaranteed by law. Personal data and commercial/industrial assets are protected under EU and constitutional law. Therefore, there must always be legal and technological measures to safeguard them. Which means that this solution must enshrine these legal safeguards within the code, and therefore the functioning of the Blockchain technology.[141]

Personal data protection is a very outstanding question nowadays.[142] Under the GDPR, as we have already seen, 'solely automated data processing' is forbidden. This is a risk that could be met in public procurement procedure running in a Blockchain solution. There would be some stages where an automated decision could be made regarding economic operators: for instance, concerning evaluating the existence of exclusion grounds. Some of them could probably be verified in an automated way whenever they

[141] Referring this option, recognising nevertheless the difficulty to deploy it, Nini Rose Moru. 2018. 'Blockchain Can and Will End Public Procurement Corruption'. Retrieved 5 December 2018 https://en.decentral.news/public-procurement-blockchain/.

[142] Expressly referring that 'the application of EU data protection law to blockchain-based platforms raises difficult questions', Bacon, Michels, Millard and Singh, 'Blockchain Demystified' (n 30).

are set out in precise legal terms.[143] It is the case of taxes or social security debts, even though in some legal systems, like the Portuguese, if there is a judicial dispute regarding taxes with given guarantee, it is considered that there is no debt. But, on the other hand, some other grounds of exclusion imply the discretionary decision of the contracting authority and even the possibility of running the self-cleaning process. Therefore, solely the habilitation phase poses two questions. First, not all foreseen grounds of exclusion could dismiss human intervention: a part of it could run automated; another part could not. Secondly, the exclusion grounds, when applied, have relevant effects on tenderers. Almost the same reasoning can be made, earlier, in the tender's evaluation stage, regarding the grounds to exclude the proposals. The foreseen grounds to exclude proposals are not drawn with the same precision; for some, an automated decision could be made, for others not.

In the given examples, the exclusion (either of the proposal or the chosen tenderer) made in a solely automated process effectively falls under article 22 (1) as it produces the effect of hindering the continuance in the public procedure and eventually becoming the contractual partner of the contracting authority. This is a legal effect. Of course, one must verify if the exceptions foreseen in Article 22 (2) are applicable: if the parties are entering into (or performance of) a contract between the data subject and the controller; if the process is authorised and the data subject's rights are safeguarded, and if is there consent.[144]

[143] See above the question of automated processes and GDPR.

[144] For further details on the exceptions, Finck, 'Blockchain and Data Protection in the European Union' (n 18) 1 at 11 ff. This last possibility generates several questions regarding the extent of the information, i. e. who the responsible for giving the information is, considering the blockchain underneath, and so on.

Secondly, and leaving behind the first and determinant issue of being an automated process, one must reflect upon the specific procedure requirements within public procurement regarding the tender's evaluation. The key factor in evaluation is the award criterion, which is an important dimension to achieve 'sustainable procurement'.

The concept of 'sustainable procurement' is very uncertain and difficult. For long a time, some other and partial expressions such as 'social clause', 'fair procurement', 'ethical procurement', and 'green procurement' were used instead. The concept of sustainability itself is connected with public procurement, mainly related to the implementation of green and social policies. This context partially explains why Christopher McCrudden wonders if the umbrella concept [sustainable procurement] helps understand 'the commodities of social and green public purchasing or serve[s] only to camouflage their essential differences'.[145] Sustainability, however, has been a constant concern in the European Union, and it has already been established in article 11 of the Treaty on the Functioning of the European Union ('TFEU'). But it is with the Lisbon 2020 Strategy – A strategy for smart, sustainable and inclusive growth[146] – which has elected sustainability as one of the most important goals for its 'vision of Europe's social market economy for the 21st century', that the issue has gained more visibility. Focusing on sustainable growth as a particular domain of sustainability, the Commission aims to 'promot[e] a more resource efficient, greener and more competitive economy'. Therefore, the 2020 Strategy foresees the development of 'new processes and technologies, including green technologies, accelerating the roll out of smart grids using ICTs, exploiting EU-scale networks, and reinforcing the competitive advantages of our businesses, particularly in manufacturing

[145] Christopher McCrudden, 'Using public procurement to achieve social outcomes', *Natural Resources Forum* 28 (2004) 257 at 266.

[146] Communication from the Commission Europe 2020 (COM/2010/2020 final) 3 March 2010. Retrieved http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.

and within our SMEs, as well through assisting consumers to value resource efficiency. Such an approach will help the EU to prosper in a low-carbon, resource constrained world while preventing environmental degradation, biodiversity loss and unsustainable use of resources. It will also underpin economic, social and territorial cohesion'.

Public procurement has always been set out as a primary instrument to promote the Internal Market in a preferentially economic feature. However, since the 2004 Directives, the European legislator has been assuming broader purposes for public procurement. Public contracts may and should be used by Member States to promote the initially secondary, nowadays horizontal policies as well, namely environmental and social ones.

Still, it is also important to enshrine other prominent features within this broad concept such as IT, with the fostering of e-procurement, and small enterprises' policy access to procurement market, which is why it is now important to use the 'sustainable procurement' concept, as public procurement contributes to 'global sustainability: balancing of social and economic development, ensuring the fundamentals of equality of life for all people, within the ecological boundaries of the planet'. Sustainable procurement should not be confused with green public procurement, as the first 'also emphasizes concern for the social and economic aspects of procurement'. In the same path, the United Nations have already proclaimed that 'sustainable Procurement seeks to achieve the appropriate balance between the three pillars of sustainable development i.e. economic, social and environmental'. Nevertheless, it is important to emphasise that 'the European Commission describes sustainable procurement as a policy instrument that relies on market dynamics rather than the law'. Besides, the concept of sustainable procurement is very workable within the Circular Economy Policy the European Union has also been embracing. And the Life Cycling Cost factor (LCC) within the award criterion gives a major contribution to build and deepen it. In its COM (2015) 614 final Communication of 2/12/2015, the Commission stated that ‘by stimulating activity in key sectors and new business opportunities […] under the umbrella of EU’s Horizon 2020 […] there are comprehensive commitments in several areas including public procurement’. And that ‘Public procurement accounts for a large proportion of European consumption (nearly 20% of EU GDP). It can therefore play a key role in the circular economy, and the Commission will encourage this role through its actions on Green Procurement’.

As Dacian Dragos/Bogdana Neamtu stress, creating ‘an umbrella framework to green and social public procurement is far more complicated’. [147] And Oshani Perera poses the following question: ‘in the rush to stimulate ‘quick wins’ and flagship initiatives to promote sustainable public procurement, are governments overlooking the critical importance of demonstrating ‘value for money’ and the business case for sustainable public procurement?’, concluding that ‘without LCC methodologies to demonstrate this, SPP policies run the risk of being side lined or even abandoned on the premise that sustainable goods and services are more expensive’. And wonders if ‘procurers and sustainable procurement policy-makers have the expertise to interpret LCC analyses to demonstrate the value for the public purse’.[148]

Two of the legal instruments used in the 2014 Directives to pursue sustainable procurement were technical specifications and award criteria rules. Within the latter, the life-cycle costing factor appears as a significant factor to appraise the proposal’s cost.[149]

[147] Dacian Dragos and Bogdana Neamtu, ‘Life-Cycle Costing for Sustainable Public Procurement in the European Union’, in: Beate Sjäfjell and Anya Wiesbrock (eds.), *Sustainable Public Procurement under EU Law – New Perspectives on the State as Stakeholder* (Cambridge University Press, 2016) 116.

[148] Oshani Perera, ‘Life Cycle Costing in Sustainable Public Procurement: A Question of Value’, International Institute for Sustainable Development (IISD) December 2009, 3

[149] Both concepts (sustainable procurement and life-cycle costing) are non-legal, interdisciplinary concepts, turning its content far more complex.

According to the 2014 Directives, we can state that the contract award criterion is ‘the most economically advantageous tender’ in a multifactorial model or in a single factorial model (best price). Depending on the contract object and its complexity, contracting authorities choose the award criteria. The object contract is also determinant to the larger or smaller degree of clauses’ complexity. The MEAT criterion, with its multiple factors, is a better tool to assess several features of the procedure and favours the pursuit of sustainability by demanding from the market solutions regarding less energy consumption goods, low carbon solutions, ecolabel products, the implementation of social policies regarding disability employment, social services, or fair commerce. All these requirements are very demanding in what concerns the MEAT criterion design and its evaluation.

The simplest award criterion is the best price, as it can be related to a simple mathematic comparison. Whenever the MEAT criterion is used, EU law imposes the display of the graduation formula, with the factor’s weight clearly explained, before the period of proposals presentation. Not all the factors are mathematically described, though. As regards those displayed in a formula, it could be easier to translate them into software code. But, if technical specifications are drawn in a discretionary way, embedding concepts such as quality measures or adequate measures, that formula needs human intervention. Or, if the formula establishes an evaluation frame, with a gap, there has to be a human decision accompanied by reasoning. All these determinations make the use of Blockchain technology harder.

For now, and within the scope of the Directives, EU Member States have to comply with the award rules. The Public Procurement Directives allow a discretionary transposition of those rules, but there are also some significant boundaries that confine the extent of different rules. For instance, award criteria that favour national economic operators or do not respect cross-border competition must be put aside. Therefore, some experiences of Northern European countries regarding alternative ways of procurement methods must be closely addressed within Directives provisions. Those methods can be related to the organisational bodies involved in evaluation such as external juris or assessment committees (which must nevertheless obey procurement procedures rules concerning assessment);[150] but the methods can be innovative ones, not foreseen in the Directives, such as Best Value Procurement (concessions)[151] or societal contracting.[152]/[153]

Some of the innovative features of BVP (or, at least similar ones) can actually be found in the present Public Procurement Directives: the consideration of past performance (in order to exclude economic operators)[154]; preliminary market consultations as an important tool in the preparation phase;[155] competitive dialogue, where the solution to the public authority is being built with the economic operators selected; and innovation partnerships.[156]

[150] This kind of organisational dimension could eventually function within blockchain technology and some of its features, namely the trust-built, could be very useful. Whenever, the context of human intervention broadens, the risk of discrimination or/and corruption grows.

[151] BVP solution was developed in United States and it has been used in the Netherlands. It aims to increase the project 'by mitigating risks and increasing the transparency by underscoring the pre-award phase'. (Arnoud Storteboom, Paulus Wondimu, Jardar Lohne and Ola Laedre, 'Best Value Procurement – The Practical Approach in The Netherlands', *Procedia Computer Science* 121 (2017) 398). Economic operators are asked to help the contracting authority in the identification of the risks throughout the procedure chain. It is said that this method reduces 'complexity, duration and cost while increasing the quality', by using the vendor's expertise ('*ibid* 398 at 400). So, 'changes the procurement agent's role from being the guardian over the award of a contract, to a facilitator of the delivery of expert services' (Jeroen van de Rijt, Sicco C. Santema, 'The Best Value Approach in the Netherlands: A Reflection on Past, Present and Future', *Journal for the Advancement of Performance Information and Value* 4(2) (2012) 147). The designed procedure embodies some automated processes. Presenting a matrix with the full explanation of the BVP method, Storteboom, Wondimu, Lohne and Laedre, 'Best Value Procurement – The Practical Approach in The Netherlands' (n 150) 398 at 402). For an analysis in the road construction sector, Narmo M.,Wondimu P.A, Lædre O. 'Best Value Procurement (BVP) in a Mega Infrastructure Project', in: González, V.A. (ed.), Proc. 26th Annual Conference of the International. Group for Lean Construction (IGLC), Chennai, India, 33.

[152] 'A type of public procurement in which citizens are given the opportunity to be involved in the performance of the project' ('Towards a coherent and efficient legal framework for public procurement law', Public Procurement Research Centre. Retrieved http://www.pprc.eu/english/research/).

[153] These are two examples of new ways in research fields within public procurement.

[154] Article 57 (4), g) of the 2014/24/EU Directive.

[155] Article 40 of the 2014/24/EU Directive.

[156] Article 31 of the 2014/24/EU Directive.

Finally, is the ‘smart contract’ a useful, workable tool within public procurement, namely regarding contract execution?

Although in public procurement within the European Union it is possible to harmonise some ground rules about contract law (mainly in contract formation and now with a few rules concerning public contracts execution), that possibility does not present itself in other contractual areas. This impossibility relates mainly to the different States’ legal framework, historically determined.[157]

In public procurement, a harmonisation effort is being made regarding procedure rules. But the provisions that regulate the parties’ obligations have always been a matter of national discretion. However, the latest Public Procurement Directives have included some rules concerning the execution of public contracts. Nevertheless, one must bear in mind that the reasoning beneath that legislative option is related to competition issues, not having any intention to harmonise contractual rules.

Therefore, in some cases, smart contracts (or part of them) can fall under Article 22 (1) of GDPR, because there are decisions made solely by automated process with significant effects to subjects. [158]

Hence, applying Blockchain technology to public procurement must be accompanied by personal data safeguards.

This contextualization explains the so-called ‘Sophisticated Smart Contracts’: they depend on law ‘for recognition, and conversely, large-scale adoption’, and the arbitration clause could be an instrument ‘towards GDPR compliance’.[159]

[157] However, the effort made by European Union regarding Private law must be stressed with ‘Principles, Definitions and Model Rules of European Private Law Draft Common Frame of Reference (DCFR)’, always pulled by the legal force of Directives.

[158] Finck, ‘Blockchain and Data Protection in the European Union’ (n 18) 1 at 28.

[159] Finck, ‘Blockchain and Data Protection in the European Union’ (n 18) 1 at 24 ff.

Regarding public contract execution, and bearing in mind the procedure rules, I can only foresee supply public contracts as a possibility. This kind of contracts can have very simple clauses and/or the contracting authority can fully describe the supply good features in the procedure documents, which means that the only requirement under competition is the price. This is, in my opinion, the most suitable scenario for a smart contract execution. Not only the remaining clauses ought to be very simple, but the execution conditions as well, in order to, first of all, be translated into code. Hence, only a few public contracts, namely simple supply contracts, with all specifications very literally drawn, could allow a Blockchain performance. But even then, data protection issues could arise.

So, smart contracts are not a useful tool for work contracts or concessions.[160] Those contracts have very complex legal rules to comply with, the technical specifications are not translatable into programming code as they lack the traditional logic enshrined in programming language, and their execution lingers in time. This lingering could imply contract modifications regarding a change of circumstances, or to accommodate the best public interest pursuit, and not all of them are previously predictable, nor translatable into software code.

5. Conclusion

Blockchain technology provides a set of interesting features for public procurement procedures. In abstract terms, it can be used both in public procurement procedures and contract execution. However, to implement such a possibility, some drawbacks must be addressed. It is difficult to turn most of the law provisions into code language, and, when

[160] Primavera Di Filippi and Aaron Wright also recognise that smart contracts '– at least for the immediate future – will not be able to account for these more open-ended rights and obligations, which are neither binary nor highly formulaic' (Di Filippi and Wright, *Blockchain and the Law – The Rule of Code* (n 2) 77). They were analysing contracts outside public procurement, but their conclusion is perfectly suitable within our reflexion.

that is possible, they are not fully workable. It is necessary to grant the protection of Fundamental rights concerning personal data, intellectual property and commercial and industrial secrets (patents). The banishment of human interference in public procurement procedures may seem the needed instrument to solve corruption issues in public procurement, but, considering the complexity of public contracts, also visible in the public procurement procedure, it is impossible to totally banish human intervention. Furthermore, it is not possible to choose one single kind of Blockchain. The public procurement complexity appears to suggest that a permissioned solution combined with other oracles solutions could be the best option. One must bear in mind that when it comes to open public procedures, there should be initial open access, which should be closed (and only accessible to tenderers and contracting authorities) when the proposal’s deadline presentation ends and remain like this until contract conclusion. Then, broader publicity would be needed again for community knowledge.

Despite the possibility to address some of the actual problems concerning the use of electronic platforms, as the present technology used in public procurement, Blockchain still presents some real constraints.

The world is evolving, and technology is unstoppable. Law and technology must be development partners. Yet, here, we are just starting the path!